Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
1.1.1	Computer Security Management and Culture	IT Roles and Responsibilities	Are controls such as separation of duties, least privilege, and individual accountability incorporated into all IT operations?	NIST SP 800-18	Is there a policy that requires controls such as separation of duties, least privilege, and individual accountability be incorporated into all IT operations?	Are there procedures for incorporating controls such as separation of duties, least privilege, and individual accountability incorporated into all IT operations?	Are controls such as separation of duties, least privilege, and individual accountability incorporated into all IT operations?	Have tests been successfully conducted to verify that roles and responsibilities are indeed separate and that a single individual does not have the capability to perform multiple roles and responsibilities?	Is separation of roles and responsibilities generally accepted as the way in which the organization does business and not challenged or defeated in purpose?
1.1.2	Computer Security Management and Culture	IT Roles and Responsibilities	Are security roles defined, and are they assigned to individuals (i.e., SA/NA, ISSO)?	NIST SP 800-18	Is there a policy that requires security roles be defined and assigned to individuals (i.e., SA/NA, ISSO)?	Are there procedures for defining security roles and assigning those roles to individuals (i.e., SA/NA, ISSO)?	Are security roles defined, and are they assigned to individuals (i.e., SA/NA, ISSO)?	Is verification performed to ensure security roles are appropriately defined and assigned?	Is definition and assignment of security roles a generally accepted way of doing business?
1.1.3	Computer Security Management and Culture	IT Roles and Responsibilities	Are sensitive functions divided among different individuals (i.e. key personnel and job functions like Sys. Admins or Financial Admins. etc.)?	FISCAM SD-1; OMB Cir A-130 App III	Is there a policy that requires sensitive functions be divided among different individuals (i.e. key personnel and job functions like Sys. Admins or Financial Admins. etc.)?	Are there procedures for dividing sensitive functions among different individuals (i.e. key personnel and job functions like Sys. Admins or Financial Admins. etc.)?	Are sensitive functions divided among different individuals (i.e. key personnel and job functions like Sys. Admins or Financial Admins. etc.)?	Is the division of sensitive functions among different individuals (i.e. key personnel and job functions like Sys. Admins or Financial Admins. etc.) reviewed periodically to ensure the division is appropriate?	Is the division of sensitive functions among different individuals (i.e. key personnel and job functions like Sys. Admins or Financial Admins. etc.) an accepted part of doing business?
1.1.4	Computer Security Management and Culture	IT Roles and Responsibilities	Are distinct systems support functions performed by different individuals (i.e. Sys Admins / Network Admins etc.)?	NIST SP 800-18; FISCAM SD-1; OMB Cir A-130 App III	Is there a policy that requires distinct systems support functions be performed by different individuals (i.e. Sys Admins / Network Admins etc.)?	Are there procedures for identification of distinct systems support functions and assignment to different individuals (i.e. Sys Admins / Network Admins etc.)?	Are distinct systems support functions performed by different individuals (i.e. Sys Admins / Network Admins etc.)?	Are the systems support functions performed by different individuals (i.e. Sys Admins / Network Admins etc.) periodically reviewed to ensure that they are distinct?	Is the systems support functions performed by different individuals (i.e. Sys Admins / Network Admins etc.) an accepted part of doing business?
1.1.5	Computer Security Management and Culture	IT Roles and Responsibilities	Is there separation of duties between security personnel who administer the access control function and those who administer the audit trail?	NIST SP 800-18	Is there a policy that requires separation of duties between security personnel who administer the access control function and those who administer the audit trail?	Are there procedures for establishing and maintaining separation of duties between security personnel who administer the access control function and those who administer the audit trail?	Is there separation of duties between security personnel who administer the access control function and those who administer the audit trail?	Is the separation of duties between security personnel who administer the access control function and those who administer the audit trail periodically reviewed and verified?	Is the separation of duties between security personnel who administer the access control function and those who administer the audit trail an accepted part of doing business?
1.1.6	Computer Security Management and Culture	IT Roles and Responsibilities	Are organizational structure and management authorities and responsibilities aligned?	Clinger Cohen; GISRA; GPEA; PRA; FISCAM SP-3.1	Is there a policy that requires organizational structure and management authorities and responsibilities be aligned?	Are there procedures for aligning organizational structure and management authorities and responsibilities?	Are organizational structure and management authorities and responsibilities aligned?	Does a third party periodically assess the alignment of organizational structure and management authorities?	Is the alignment of organizational structure and management authorities an accepted part of doing business?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
1.1.7	Computer Security Management and Culture	IT Roles and Responsibilities	Are key program functions identified and divided among specific roles?	GISRA	Is there a policy that requires identification of key program functions and division among specific roles?	Are there procedures for identification of key program functions and division among specific roles?	Are key program functions identified and divided among specific roles?	Are the key program functions and division among specific roles periodically reviewed and verified?	Is the identification of key program functions and division among specific roles an accepted way of doing business?
1.1.8	Computer Security Management and Culture	IT Roles and Responsibilities	Are all programs this high-risk program interfaces with identified?	GISRA	Is there a policy that requires identification of all programs this high-risk program interfaces with?	Are there procedures for identification of all programs this high-risk program interfaces with?	Are all programs this high-risk program interfaces with identified?	Are the program interfaces with this high-risk program periodically reviewed and verified?	Is the identification of all programs this high-risk program interfaces with a generally accepted way of doing business?
1.2.1	Computer Security Management and Culture	Review of Security Controls	Have security controls of each system and interconnected systems been reviewed?	FISCAM SP-5; NIST SP 800-18; OMB Cir A-130 App III	Is there a policy that requires review and verification of each of the security controls of the system and interconnected systems?	Are there procedures for review and verification of the security controls of each system and interconnected systems?	Have security controls of each system and interconnected systems been reviewed?	Has verification of security controls been confirmed?	Is the review and verification of the security controls of each system and interconnected systems performed on a regular basis without question?
1.2.2	Computer Security Management and Culture	Review of Security Controls	Has each system been subjected to periodic reviews?	FISCAM SP-5.1; OMB Cir A-130 App III	Is there a policy that requires periodic reviews of agency systems?	Are there procedures for conducting periodic reviews of agency systems?	Has each system been subjected to periodic reviews?	Is there a third party review of the periodic system reviews? If so, are the recommendations followed?	Are summary results of periodic reviews incorporated into the capital budgeting process and system portfolio reviews?
1.2.3	Computer Security Management and Culture	Review of Security Controls	Has an independent review been performed for each system in the past three years or when a significant change occurred?	FISCAM SP-5.1; NIST SP 800-18; OMB Cir A-130 App III	Is there a policy that requires an independent review be performed for each system in the past three years or when a significant change occurred?	Are there procedures for conducting independent reviews for each system in the past three years or when a significant change occurred?	Has an independent review been performed for each system in the past three years or when a significant change occurred?	Has each independent review of each system resulted in improvements to the system?	Is conducting independent reviews for each system every 3 years or when a significant change occurs an accepted way of doing business?
1.2.4	Computer Security Management and Culture	Review of Security Controls	Has the operating system been periodically reviewed to ensure the configuration prevents circumvention of the security software and application controls?	FISCAM SS-1.2; OMB Cir A-130 App III	Is there a policy that requires a periodic review of the operating system to ensure the configuration prevents circumvention of the security software and application controls?	Are there procedures for conducting a periodic review of the operating system to ensure the configuration prevents circumvention of the security software and application controls?	Has the operating system been periodically reviewed to ensure the configuration prevents circumvention of the security software and application controls?	Have tests been conducted to ensure the operating system configuration prevents circumvention of the security software and application controls?	Is conducting periodic reviews of the operating system to ensure the configuration prevents circumvention of the security software and application controls an accepted way of doing business?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
1.2.5	Computer Security Management and Culture	Review of Security Controls	Does management ensure that corrective IT security actions are effectively implemented?	NIST SP 800-18	Is there a policy that requires management to effectively implement IT security actions?	Are there procedures for management to effectively implement corrective IT security actions?	Does management ensure that corrective IT security actions are effectively implemented?	Does an independent third party periodically review the implementation of corrective IT security actions?	Is management's implementation of corrective IT security actions generally effective?
1.2.6	Computer Security Management and Culture	Review of Security Controls	Are security controls consistent with and an integral part of the IT architecture of the agency?	OMB Cir A-130 App III 8B3	Is there a policy that requires security controls be consistent with and an integral part of the IT architecture of the agency?	Are there procedures for ensuring that security controls be consistent with and an integral part of the IT architecture of the agency?	Are security controls consistent with and an integral part of the IT architecture of the agency?	Is there a periodic review of security controls to ensure they are consistent with and an integral part of the IT architecture of the agency?	Are the security controls generally verified to be consistent with and an integral part of the IT architecture of the agency?
1.2.7	Computer Security Management and Culture	Review of Security Controls	Does management initiate prompt action to correct deficiencies and is the action successful?	OMB Cir A-130 App III; NIST SP 800-18	Is there a policy that requires management to initiate prompt action to correct deficiencies?	Are there procedures for management to initiate prompt action to correct deficiencies?	Does management initiate prompt action to correct deficiencies and is the action successful?	Do periodic reviews indicate that management initiates prompt action to correct deficiencies and is generally successful?	Is management prompt action to correct deficiencies a basic part of doing business and is the action largely successful?
1.2.8	Computer Security Management and Culture	Review of Security Controls	Are access scripts with embedded passwords prohibited?	NIST SP 800-18	Is there a policy that prohibits access scripts with embedded passwords?	Are there procedures for prohibiting access scripts with embedded passwords?	Are access scripts with embedded passwords prohibited?	Are tests conducted to verify that access scripts with embedded passwords cannot be used?	Is it generally accepted and part of practice that access scripts with embedded passwords are not permitted?
1.2.9	Computer Security Management and Culture	Review of Security Controls	Is emergency and temporary access properly authorized?	FISCAM AC-2.2	Is there a policy that requires proper authorization of emergency and temporary access?	Are there procedures for proper authorization of emergency and temporary access?	Is emergency and temporary access properly authorized?	Is the proper authorization of emergency and temporary access periodically tested?	Is emergency and temporary access properly authorized as verified through testing and is this generally accepted as a way of doing business?
1.2.10	Computer Security Management and Culture	Review of Security Controls	Are audit trails reviewed frequently and identified issues acted upon?	NIST SP 800-18	Is there a policy that requires audit trails be reviewed frequently and identified issues acted upon?	Are there procedures for reviewing audit trails and acting upon identified issues?	Are audit trails reviewed frequently and identified issues acted upon?	Is there a periodic third party review of audit trails to verify that all issues were identified and to verify that those actions were acted upon?	Review of audit trails and acting on identified issues is integrated into the overall security program.

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
1.2.11	Computer Security Management and Culture	Review of Security Controls	Are automated tools used to review audit records in real time or near real time?	NIST SP 800-18	Is there a policy that requires use of automated tools to review audit records in real time or near real time?	Are there procedures for using automated tools to review audit records in real time or near real time?	Are automated tools used to review audit records in real time or near real time?	Is the automated tool review of audit records periodically verified to ensure that appropriate issues are being identified?	Is the use of automated tools to review audit records in real time or near real time effective and an accepted part of doing business?
1.2.12	Computer Security Management and Culture	Review of Security Controls	Have security controls for the program and interconnected systems been reviewed?	OMB Cir A-130 App III; GISRA	Is there a policy that requires review of security controls for the program and interconnected systems?	Are there procedures for reviewing security controls for the program and interconnected systems?	Have security controls for the program and interconnected systems been reviewed?	Has the review of security controls for the program and interconnected systems been verified by an independent third party?	Are the security controls for the program and interconnected systems appropriate and do they prevent compromise?
1.2.13	Computer Security Management and Culture	Review of Security Controls	Has the program been subjected to periodic reviews?	OMB Cir A-130 App III; GISRA	Is there a policy that requires periodic program reviews?	Are there procedures for conducting periodic program reviews?	Has the program been subjected to periodic reviews?	Are the periodic program reviews examined and verified by an independent third party?	Are periodic program reviews effective and an accepted way of doing business?
1.3.1	Computer Security Management and Culture	Rules of Behavior and Documentation	If security controls are added or modified, is the system documentation updated to include them?	OMB Cir A-130 App III; NIST SP 800-18	Is there a policy that requires system documentation update when security controls are added or modified?	Are there procedures for updating system documentation when security controls are added or modified?	If security controls are added or modified, is the system documentation updated to include them?	Is system documentation periodically reviewed to ensure current security controls are documented?	Is system documentation of current security controls the general accepted practice?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
1.3.2	Computer Security Management and Culture	Rules of Behavior and Documentation	Have Rules of Behavior been established by the organization, acknowledged by users via signature, and enforced?	OMB Cir A-130 App III; NIST SP 800-18	Is there a policy that requires establishment of Rules of Behavior, user acknowledgment of those rules via signature, and enforcement of those rules?	Are there procedures for establishing and enforcing Rules of Behavior and for obtaining user acknowledgment of those rules via signature?	Have Rules of Behavior been established by the organization, acknowledged by users via signature, and enforced?	Have the established Rules of Behavior been periodically reviewed to ensure they are appropriate for current conditions? Has user acknowledgment been verified for all users? Is there periodic review to ensure enforcement of the rules?	Are the established Rules of Behavior generally appropriate for current conditions? Have all users acknowledged those rules and generally follow them without question?
1.3.3	Computer Security Management and Culture	Rules of Behavior and Documentation	Is illegal use of copyrighted software or shareware prevented?	NIST SP 800-18	Is there a policy that forbids illegal use of copyrighted software or shareware?	Are there procedures for preventing illegal use of copyrighted software or shareware?	Is illegal use of copyrighted software or shareware prevented?	Are measures taken to ensure no illegal use of copyrighted software or shareware?	Is illegal use of copyrighted software or shareware extremely rare and considered to be against business practices?
1.3.4	Computer Security Management and Culture	Rules of Behavior and Documentation	Is the use of copyrighted software or shareware and personally owned software/equipment documented?	NIST SP 800-18	Is there a policy that requires documentation of the use of copyrighted software or shareware and personally owned software/equipment?	Are there procedures for documenting the use of copyrighted software or shareware and personally owned software/equipment?	Is the use of copyrighted software or shareware and personally owned software/equipment documented?	Are periodic reviews performed to verify that all use of copyrighted software or shareware and personally owned software/equipment is documented?	Is documentation of the use of copyrighted software or shareware and personally owned software/equipment generally accepted practice? Is all use documented?
1.3.5	Computer Security Management and Culture	Rules of Behavior and Documentation	Is password use appropriate?	NIST SP 800-18	Is there a policy that defines appropriate password use?	Are there procedures for appropriate password use?	Is password use appropriate?	Is password use verified to be appropriate?	Is appropriate password use a part of the business practice?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
1.3.6	Computer Security Management and Culture	Rules of Behavior and Documentation	Is there sufficient documentation that explains how software/hardware is to be used?	OMB Cir A-130 App III 8B3	Is there a policy that requires documentation sufficient to explain how software/hardware is to be used?	Are there procedures for development of or acquisition of documentation sufficient to explain how software/hardware is to be used?	Is there sufficient documentation that explains how software/hardware is to be used?	Is the software/hardware documentation periodically reviewed to ensure that it explains how software/hardware is to be used? Are the users asked to provide input?	Is documentation generally sufficient to explain how software/hardware is to be used? Is this accepted practice?
1.3.7	Computer Security Management and Culture	Rules of Behavior and Documentation	Are there procedures to be followed in case of emergency?	NIST SP 800-18	Is there a policy that requires development of procedures to be followed in case of emergency?	Are there procedures for development of procedures to be followed in case of emergency?	Are there procedures to be followed in case of emergency?	Have the emergency procedures been tested?	Are the emergency procedures well understood and used by employees? Are they effective?
1.3.8	Computer Security Management and Culture	Rules of Behavior and Documentation	Are IT systems backed up periodically?	NIST SP 800-18	Is there a policy that requires IT systems to be backed up periodically and is the frequency established?	Are there procedures for IT systems to be backed up periodically?	Are IT systems backed up periodically?	Are IT system backups verified to be complete and at the appropriate frequency of occurrence for each IT system? Have the backups been periodically tested to ensure complete recovery is possible?	Are all IT system backups complete and performed at the appropriate frequency of occurrence for each IT system? Are IT systems capable of complete recovery? Is IT system backup an accepted part of doing business?
1.3.9	Computer Security Management and Culture	Rules of Behavior and Documentation	Are formal security and operational procedures implemented?	NIST SP 800-18	Is there a policy that requires use of formal security and operational procedures?	Are there procedures for development and use of formal security and operational procedures?	Are formal security and operational procedures implemented?	Have the formal security and operational procedures been tested and shown to be effective?	Are the formal security and operational procedures effective and incorporated into general practice?
1.3.10	Computer Security Management and Culture	Rules of Behavior and Documentation	Are lost and compromised passwords handled correctly?	NIST SP 800-18; FISCAM AC-3.2	Is there a policy that requires lost and compromised passwords to be handled in a specific manner?	Are there procedures for handling of lost and compromised passwords?	Are lost and compromised passwords handled correctly?	Is there a verification that lost and compromised passwords are handled correctly? Has a test of social engineering principles been used to determine if someone can gain access to a password to which they are not entitled?	Is correct handling of lost and compromised passwords a basic part of the accepted business practice (social engineering does not work)?
1.3.11	Computer Security Management and Culture	Rules of Behavior and Documentation	Are passwords distributed securely and users informed not to reveal their passwords to anyone (social engineering)?	NIST SP 800-18; FISCAM AC-3.2	Is there a policy that requires secure handling and distribution of passwords?	Are there procedures for secure handling and distribution of passwords?	Are passwords distributed securely and users informed not to reveal their passwords to anyone (social engineering)?	Is the secure distribution and handling of passwords periodically tested?	Is secure distribution and handling of passwords a basic part of doing business?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
1.3.12	Computer Security Management and Culture	Rules of Behavior and Documentation	Is an approved standardized log-on banner displayed on the system warning unauthorized users that they have accessed a U.S. government system and can be punished for inappropriate use?	NIST SP 800-18; FISCAM AC-3.2	Is there a policy that requires an approved standardized log-on banner be displayed on the system warning unauthorized users that they have accessed a U.S. government system and can be punished for inappropriate use?	Are there procedures for use of an approved standardized log-on banner?	Is an approved standardized log-on banner displayed on the system warning unauthorized users that they have accessed a U.S. government system and can be punished for inappropriate use?	Is there periodic verification that all access to the systems results in display of an approved standardized log-on banner warning unauthorized users that they have accessed a U.S. government system and can be punished for inappropriate use?	Is there always a display of an approved standardized log-on banner warning unauthorized users that they have accessed a U.S. government system and can be punished for inappropriate use upon access to all systems? Is this recognized as a standard way of doing business?
1.3.13	Computer Security Management and Culture	Rules of Behavior and Documentation	Is a privacy policy posted on each web site?	Privacy Act of 1974	Is there a policy that requires posting of a privacy policy on each web site?	Are there procedures for posting a privacy policy on each web site?	Is a privacy policy posted on each web site?	Are tests periodically run to verify that a privacy policy is posted on each web site?	Is it generally accepted practice that a privacy policy is posted on each web site?
1.4.1	Computer Security Management and Culture	Performance Assessment and Feedback	Have routine self-assessments (peer reviews and the like) been conducted in the past three years?	NIST SP 800-18; OMB Cir A-130 App III	Is there a policy that requires routine self-assessments (peer reviews and the like) be conducted every three years?	Are there procedures for conducting routine self-assessments (peer reviews and the like) every three years?	Have routine self-assessments (peer reviews and the like) been conducted in the past three years?	Have the routine self-assessments (peer reviews and the like) been reviewed by an independent third party to verify the accuracy of the assessment?	Are the routine self-assessments (peer reviews and the like) accurate? Do they result in corrective action? Is the corrective action shown to improve the situation?
1.4.2	Computer Security Management and Culture	Performance Assessment and Feedback	Are tests and examinations of key security controls routinely conducted (i.e., network scans, analyses of router and switch setting, penetration testing)?	NIST SP 800-18; OMB Cir A-130 App III 8B3	Is there a policy that requires conducting tests and examinations of key security controls routinely (i.e., network scans, analyses of router and switch setting, penetration testing)?	Are there procedures for conducting tests and examinations of key security controls routinely (i.e., network scans, analyses of router and switch setting, penetration testing) that include the nature, extent, and timing of the tests and examinations?	Are tests and examinations of key security controls routinely conducted (i.e., network scans, analyses of router and switch setting, penetration testing)?	Are there periodic reviews of the tests and examinations of key security controls routinely conducted to ensure the tests are appropriate?	Are the tests and examinations of key security controls part of the general mechanism of doing business?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
1.4.3	Computer Security Management and Culture	Performance Assessment and Feedback	Are security alerts and security incidents analyzed and remedial actions taken?	FISCAM SP-3.4; NIST SP 800-18; OMB Cir A-130 App III	Is there a policy that requires analysis of security alerts and security incidents? Is the severity of alerts & incidents specified by category?	Are there procedures for analysis of security alerts and incidents? Are there procedures for determination of corrective action and its implementation? Do the procedures specify the timing and nature of the remedial action to be taken for each category of incident and alert?	Are security alerts and security incidents analyzed and remedial actions taken?	Are the security alert and incident analyses and remedial actions taken periodically reviewed and verified by an independent third party?	Are the security alert and incident analyses and remedial actions taken generally appropriate? Are improvements made as a result? Is this activity part of the mechanisms for doing business?
1.4.4	Computer Security Management and Culture	Performance Assessment and Feedback	Are significant IT security weaknesses reported and effective remedial action taken?	FISCAM SP-5.1; NIST SP 800-18; OMB Cir A-130 App III	Is there a policy that requires reporting significant IT security weaknesses and taking effective remedial action?	Are there procedures for identification of and reporting significant IT security weaknesses? Are there procedures for taking effective remedial action?	Are significant IT security weaknesses reported and effective remedial action taken?	Is an examination done to verify that significant IT security weaknesses are reported and effective remedial action taken?	Are all significant IT security weaknesses reported and effective remedial action taken in a timely manner? Does this result in fewer or less critical weaknesses? Is information gained incorporated into future efforts?
1.4.5	Computer Security Management and Culture	Performance Assessment and Feedback	Are the tracking, escalating, and closing of corrective actions effective?	NIST SP 800-18; OMB Cir A-130 App III	Is there a policy that requires tracking, escalating, and closing corrective actions?	Are there procedures for tracking, escalating, and closing corrective actions?	Are the tracking, escalating, and closing of corrective actions effective?	Is the process for tracking, escalating, and closing corrective actions tested for its effectiveness and ability to prevent recurrence?	Is the process for tracking, escalating, and closing corrective actions an integral part of doing business? Does it result in improved IT security?
1.4.6	Computer Security Management and Culture	Performance Assessment and Feedback	Are metrics developed for the enterprise computer security program?	GISRA	Is there a policy that requires development of metrics for the enterprise computer security program?	Are there procedures for the development of metrics for the computer security program?	Are metrics developed for the enterprise computer security program?	Are the metrics that have been developed verified to be effective?	Are these metrics used in the lifecycle planning, capital planning, investment control, and budget processes?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
1.4.7	Computer Security Management and Culture	Performance Assessment and Feedback	Are computer security metrics used to track security program performance, assess the costs and benefits of security controls, and provide feedback to management?	GISRA	Does policy require computer security metrics be used to track security program performance, assess the costs and benefits of security controls, and provide feedback to management?	Are there procedures for use of security metrics to track security program performance, assess the costs and benefits of security controls, and provide feedback to management?	Are computer security metrics used to track security program performance, assess the costs and benefits of security controls, and provide feedback to management?	Is there verification that security metrics improve security program performance, and provide improved benefits, or decrease costs?	Are these metrics used in the lifecycle planning, capital planning, investment control, and budget processes?
1.5.1	Computer Security Management and Culture	Critical Infrastructure Protection	Are resources supporting critical operations identified?	FISCAM SC-1.2	Is there a policy that requires identification of resources supporting critical operations?	Are there procedures for identification of resources supporting critical operations?	Are resources supporting critical operations identified?	Are resources identified to support critical operations verified to ensure the resources are in fact supporting critical operations?	Are the resources identified effectively supporting critical operations? Is this support an integral part of doing business?
1.5.2	Computer Security Management and Culture	Critical Infrastructure Protection	Are high-risk programs identified and provided the appropriate level of management attention and resources.	OMB Cir A-130 App III; FISCAM SC-1.2	Is there a policy that requires identification of high-risk programs?	Are there procedures for identification of high-risk programs?	Are high-risk programs identified and provided the appropriate level of management attention and resources.	Is the process for identification of high-risk programs verified? Is there an assessment of the management awareness of the issues relevant to the high-risk programs? Is there an assessment of how well management is addressing those issues?	Is identification of high-risk programs an integral part of doing business? Is management aware of the issues relevant to the high-risk programs? Are the high-risk programs operating successfully?
1.5.3	Computer Security Management and Culture	Critical Infrastructure Protection	Have critical interdependencies related to critical assets/operations been identified and documented in an approved risk assessment?	PDD-63; NIST SP 800-18; FISCAM SC-1	Is there a policy that requires identification and documentation in an approved risk assessment of critical interdependencies related to critical assets/operations?	Are there procedures for identifying and documenting in an approved risk assessment critical interdependencies related to critical assets/operations?	Have critical interdependencies related to critical assets/operations been identified and documented in an approved risk assessment?	Are the critical interdependencies related to critical assets/operations verified by an independent third party?	Is identification and documentation of interdependencies related to critical assets/operations a part of doing business?
1.5.4	Computer Security Management and Culture	Critical Infrastructure Protection	Have all critical assets/operations been identified and inventoried in writing?	PDD-63; FISCAM SC-1	Is there a policy that requires that all critical assets/operations be identified and inventoried in writing?	Are there procedures for identifying and inventorying all critical assets/operations?	Have all critical assets/operations been identified and inventoried in writing?	Has the identification and inventory of critical assets/operations been verified by an independent third party?	Is the process of inventorying critical assets/operations integrated into the normal business processes of the organization?
1.5.5	Computer Security Management and Culture	Critical Infrastructure Protection	Is there a Critical Infrastructure Protection plan?	FISCAM SC-1; PDD-63	Is there a policy that requires development of a Critical Infrastructure Protection plan?	Are there procedures for developing a Critical Infrastructure Protection plan?	Is there a Critical Infrastructure Protection plan?	Has the Critical Infrastructure Protection plan been verified by an independent third party?	Is there a Critical Infrastructure Protection plan?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
1.5.6	Computer Security Management and Culture	Critical Infrastructure Protection	Have all interdependent organizations been identified and documented in Critical Infrastructure Protection plans and contingency plans?	PDD-63; NIST SP 800-18; NIST SP 800-12; FISCAM SC-1	Is there a policy that requires identification and documentation in Critical Infrastructure Protection plans and contingency plans of all interdependent organizations?	Are there procedures for identifying and documenting in Critical Infrastructure Protection plans and contingency plans all interdependent organizations?	Have all interdependent organizations been identified and documented in Critical Infrastructure Protection plans and contingency plans?	Have the Critical Infrastructure Protection plans and contingency plans been verified to ensure that all interdependent organizations are identified?	Is the identification and documentation in Critical Infrastructure Protection plans and contingency plans of all interdependent organizations an accepted business practice?
1.5.7	Computer Security Management and Culture	Critical Infrastructure Protection	Are there plans for coordinating communications and recovery operations with interdependent organizations?	PDD-63; NIST SP 800-18; NIST SP 800-12; FISCAM SC-1	Is there a policy that requires development of plans for coordinating communications and recovery operations with interdependent organizations?	Are there procedures for developing plans for coordinating communications and recovery operations with interdependent organizations?	Are there plans for coordinating communications and recovery operations with interdependent organizations?	Are the plans for coordinating communications and recovery operations with interdependent organizations verified by an independent third party?	Are there plans for coordinating communications and recovery operations with interdependent organizations?
1.5.8	Computer Security Management and Culture	Critical Infrastructure Protection	Is the Critical Infrastructure Protection plan kept current with changes in assets/operations?	FISCAM SC-1; PDD-63	Is there a policy that requires that the Critical Infrastructure Protection plan be kept current with changes in assets/operations?	Are there procedures for synchronizing the Critical Infrastructure Protection plan with changes in assets/operations?	Is the Critical Infrastructure Protection plan kept current with changes in assets/operations?	Is the Critical Infrastructure Protection plan periodically reviewed to ensure that it reflects current changes in assets/operations?	Is the synchronization of the Critical Infrastructure Protection plan with changes in assets/operations an integral part of doing business?
1.5.9	Computer Security Management and Culture	Critical Infrastructure Protection	Is the Critical Infrastructure Protection plan updated at least every two years?	FISCAM SC-1; PDD-63	Is there a policy that requires the Critical Infrastructure Protection plan be updated at least every two years?	Are there procedures for updating the Critical Infrastructure Protection plan every two years?	Is the Critical Infrastructure Protection plan updated at least every two years?	Is the Critical Infrastructure Protection plan periodically reviewed to ensure that it is updated at least every two years and reflects circumstances at that time?	Is review and update of the Critical Infrastructure Protection plan integrated into the overall business process?
1.5.10	Computer Security Management and Culture	Critical Infrastructure Protection	Have all known critical points-of-failure been identified, documented, and had mitigation plans developed for each one?	FISCAM SC-1; PDD-63	Is there a policy that requires the identification, documentation, and mitigation of critical points-of-failure?	Are there procedures for identification, documentation, and mitigation of critical points-of-failure?	Have all known critical points-of-failure been identified, documented, and had mitigation plans developed for each one?	Is there a verification of the identified critical points-of-failure? Are mitigation plans developed for each one?	Is the identification, documentation, and mitigation of critical points-of-failure integrated into the overall business process?
1.5.11	Computer Security Management and Culture	Critical Infrastructure Protection	Have all business partners developed and agreed to interconnection agreements?	FISCAM SC-1; PDD-63	Is there a policy that requires all business partners develop and agree to interconnection agreements?	Are there procedures for business partners to develop and agree to interconnection agreements?	Have all business partners developed and agreed to interconnection agreements?	Is a periodic review performed to verify that all business partners developed and agreed to interconnection agreements?	Is it part of the general business practice to engage all business partners to develop and agree to interconnection agreements?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
1.5.12	Computer Security Management and Culture	Critical Infrastructure Protection	Do interconnection agreements cover all known forms of access required on the part of both partners? Are the interconnections audited or reviewed on a regular basis to ensure appropriate usage?	FISCAM SC-1; PDD-63	Is there a policy that requires interconnection agreements to cover all known forms of access required on the part of both partners? Does the policy require that interconnections be audited or reviewed on a regular basis to ensure appropriate usage?	Are there procedures for establishing, auditing, and reviewing interconnection agreements to ensure appropriate usage?	Do interconnection agreements cover all known forms of access required on the part of both partners? Are the interconnections audited or reviewed on a regular basis to ensure appropriate usage?	Does an independent third party periodically verify interconnection agreements? Is there a process to examine the audits and reviews of the agreements to ensure they perform as expected?	Are current and correct interconnection agreements a standard part of doing business?
1.5.13	Computer Security Management and Culture	Critical Infrastructure Protection	Do interconnection agreements uniformly provide for the information security requirements of each partner?	FISCAM SC-1; PDD-63	Is there a policy that requires that interconnection agreements uniformly provide for the information security requirements of each partner?	Are there procedures for uniformly providing for the information security requirements of each partner in all interconnection agreements?	Do interconnection agreements uniformly provide for the information security requirements of each partner?	Are interconnection agreements periodically reviewed to ensure that the information security requirements of each partner are uniformly provided?	Are interconnection agreements that uniformly provide for the information security requirements of each partner part of an accepted way of doing business?
1.6.1	Computer Security Management and Culture	Personnel Controls	Are all positions reviewed for sensitivity level?	NIST SP 800-18; FISCAM SD-1.2	Is there a policy that requires review of all positions for sensitivity level?	Are there procedures for reviewing all positions for sensitivity level?	Are all positions reviewed for sensitivity level?	Are all positions periodically reviewed to ensure that sensitivity levels are appropriate and correct?	Are appropriate and correct position sensitivity levels part of an accepted way of doing business?
1.6.2	Computer Security Management and Culture	Personnel Controls	Are there documented job descriptions that accurately reflect assigned duties and responsibilities and that segregate duties?	FISCAM SD-1.2	Is there a policy that requires documented job descriptions that accurately reflect assigned duties and responsibilities and that segregate duties?	Are there procedures for documenting job descriptions that accurately reflect assigned duties and responsibilities and that segregate duties?	Are there documented job descriptions that accurately reflect assigned duties and responsibilities and that segregate duties?	Is there a periodic review of documented job descriptions to ensure that they accurately reflect assigned duties and responsibilities and that duties are segregated?	Are documented job descriptions that accurately reflect assigned duties and responsibilities and that segregate duties part of an accepted way of doing business?
1.6.3	Computer Security Management and Culture	Personnel Controls	Are mechanisms in place for holding users responsible for their IT security relevant actions?	OMB Cir A-130 App III	Is there a policy that requires mechanisms for holding users responsible for their IT security relevant actions?	Are there procedures for developing and enforcing mechanisms for holding users responsible for their IT security relevant actions?	Are mechanisms in place for holding users responsible for their IT security relevant actions?	Are the mechanisms for holding users responsible for their IT security relevant actions tested to ensure effectiveness?	Are users held responsible for their IT security relevant actions without exception? Are the consequences generally known and accepted?
1.6.4	Computer Security Management and Culture	Personnel Controls	Are regularly scheduled vacations and periodic job/shift rotations required?	FISCAM SP-4.1	Is there a policy that requires regularly scheduled vacations and periodic job/shift rotations?	Are there procedures for establishing and enforcing regularly scheduled vacations and periodic job/shift rotations?	Are regularly scheduled vacations and periodic job/shift rotations required?	Are time schedules periodically reviewed and verified to ensure that regularly scheduled vacations and periodic job/shift rotations are being adhered to?	Are regularly scheduled vacations and periodic job/shift rotations accepted and followed as part of doing business?
1.6.5	Computer Security Management and Culture	Personnel Controls	Are all IT user accounts effectively managed upon personnel hiring, transfer, and termination?	NIST SP 800-18; FISCAM SP-4.1	Is there a policy that requires appropriate training before establishing IT accounts for new hires and transfers into new positions, review of a transfer's account access with immediate termination of accounts that are not part of the new position, and other effective management of all IT user accounts?	Are there procedures for providing appropriate training before establishing IT accounts for new hires and transfers into new positions, reviewing a transfer's account access with immediate termination of accounts that are not part of the new position, and providing other effective management of all IT user accounts?	Are all IT user accounts effectively managed upon personnel hiring, transfer, and termination?	Are all IT user accounts periodically reviewed to ensure that users that should not have access to IT systems do not, and users that need and should have access to IT systems have access?	Are all IT user accounts valid and appropriate? Is IT account management performed in a timely fashion? Are IT accounts removed within 24 hours of employee termination?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
1.6.6	Computer Security Management and Culture	Personnel Controls	Is appropriate background screening for personnel completed prior to granting access to information or systems?	NIST SP 800-18	Is there a policy that requires appropriate background screening for personnel be completed prior to granting access to information or systems?	Are there procedures for completing appropriate background screening for personnel prior to granting access to information or systems?	Is appropriate background screening for personnel completed prior to granting access to information or systems?	Is there a periodic review of personnel background screening to ensure that access is not obtained prior to successful completion of background screening?	Are personnel appropriately screened before accessing information or systems? Is this generally accepted practice?
1.6.7	Computer Security Management and Culture	Personnel Controls	Are individuals who are authorized to bypass significant technical and operational controls screened prior to access and periodically thereafter?	OMB Cir A-130 App III	Is there a policy that requires screening prior to access and periodically thereafter for individuals who are authorized to bypass significant technical and operational controls?	Are there procedures for performing and evaluating screening of individuals who are authorized to bypass significant technical and operational controls?	Are individuals who are authorized to bypass significant technical and operational controls screened prior to access and periodically thereafter?	Is the screening of individuals who are authorized to bypass significant technical and operational controls periodically reviewed and validated by an independent third party?	Are individuals who are authorized to bypass significant technical and operational controls periodically appropriately screened prior to access? Is this accepted business practice?
1.6.8	Computer Security Management and Culture	Personnel Controls	Are individuals screened prior to information access when controls cannot adequately protect the information?	OMB Cir A-130 App III	Is there a policy that requires screening of individuals prior to information access when controls cannot adequately protect the information?	Are there procedures for screening of individuals prior to information access when controls cannot adequately protect the information?	Are individuals screened prior to information access when controls cannot adequately protect the information?	Is the screening of individuals prior to information access when controls cannot adequately protect the information periodically reviewed and validated by an independent third party?	Are individuals who have access to information access that cannot be adequately protected via controls appropriately screened prior to access? Is this accepted business practice?
1.6.9	Computer Security Management and Culture	Personnel Controls	Are all conditions requiring information access prior to completion of screening appropriately defined and is the information access appropriately controlled?	NIST SP 800-18; FISCAM AC-2.2; OMB Cir A-130 App III	Is there a periodic review and update of the conditions under which information access prior to completion of screening is considered necessary to ensure only appropriate information access?	Are there procedures for defining and controlling the conditions under which information access prior to completion of screening is necessary?	Are all conditions requiring information access prior to completion of screening appropriately defined and is the information access appropriately controlled?	Is there a periodic review and update of the conditions under which information access prior to completion of screening is considered necessary to ensure only appropriate information access?	Are the conditions under which information access prior to completion of screening is considered necessary relatively rare and very well defined? Is information access appropriately controlled when the conditions do arise? Is there an accepted practice to minimize the occurrence of these conditions?
1.6.10	Computer Security Management and Culture	Personnel Controls	Are there restrictions on who performs maintenance and repair activities?	NIST SP 800-18; OMB Cir A-130 App III; FISCAM SS-3.1	Is there a policy that restricts who is permitted to perform maintenance and repair activities?	Are there procedures for restricting who perform maintenance and repair activities?	Are there restrictions on who performs maintenance and repair activities?	Are the restrictions on who performs maintenance and repair activities periodically reviewed to ensure the restrictions are appropriate?	Are restrictions on who performs maintenance and repair activities part of an accepted way of doing business?
1.6.11	Computer Security Management and Culture	Personnel Controls	Is a current list of authorized users and their access maintained and approved?	NIST SP 800-18	Is there a policy that requires maintenance and approval of a current list of authorized users and their access?	Are there procedures for maintaining and approving a current list of authorized users and their access?	Is a current list of authorized users and their access maintained and approved?	Is the list of authorized users and their access periodically reviewed to ensure correctness?	Is a current list of authorized users and their access considered part of doing business?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
1.6.12	Computer Security Management and Culture	Personnel Controls	Do data owners periodically review access authorizations to ensure that they remain appropriate?	FISCAM AC-2.1	Is there a policy that requires data owners to periodically review access authorizations to ensure that they remain appropriate?	Are there procedures for reviewing access authorizations to ensure that they remain appropriate?	Do data owners periodically review access authorizations to ensure that they remain appropriate?	Are periodic reviews of access authorizations by data owners to ensure that they remain appropriate periodically verified by an independent third party?	Is periodic review by data owners of access authorizations to ensure that they remain appropriate considered a standard business practice?
1.6.13	Computer Security Management and Culture	Personnel Controls	Are guest and anonymous accounts authorized and monitored?	NIST SP 800-18	Is there a policy that requires authorizing and monitoring of guest and anonymous accounts? Are the conditions required for authorization and termination provided?	Are there procedures for authorizing and monitoring of guest and anonymous accounts?	Are guest and anonymous accounts authorized and monitored?	Are there periodic reviews of guest and anonymous accounts authorization and monitoring by an independent third party?	Are periodic reviews of guest and anonymous accounts standard business practice?
1.6.14	Computer Security Management and Culture	Personnel Controls	How is the access to information or programs assigned and removed and how is this access tracked?	OMB Cir A-130 App III; GISRA	Is there a policy that requires tracking of assigning and removing access to information or programs?	Are there procedures for tracking of assigning and removing access to information or programs?	How is the access to information or programs assigned and removed and how is this access tracked?	Are there periodic reviews of assigning and removing access to information or programs to ensure appropriate controls?	Is tracking of assigning and removing access to information or programs to ensure appropriate controls standard business practice?
1.6.15	Computer Security Management and Culture	Personnel Controls	Is enhanced screening of user access implemented for high-risk programs at appropriate intervals?	OMB Cir A-130 App III; GISRA	Is there a policy that requires periodic enhanced screening of user access to high-risk programs?	Are there procedures for periodic enhanced screening of user access to high-risk programs?	Is enhanced screening of user access implemented for high-risk programs at appropriate intervals?	Is enhanced screening of user access for high-risk programs periodically reviewed to ensure the necessary controls are in place?	Is enhanced screening of user access for high-risk programs periodically reviewed to ensure the necessary controls are in place standard business practice?
1.6.16	Computer Security Management and Culture	Personnel Controls	Is vendor/contractor access to information controlled in a fashion equivalent to or greater than Federal employee's access is controlled?	OMB Cir A-130 App III; GISRA	Is there a policy that requires vendor/contractor access to information be controlled in a fashion equivalent to or greater than Federal employee's access is controlled?	Are there procedures for controlling vendor/contractor access to information that is equivalent to or greater than Federal employee's access is controlled?	Is vendor/contractor access to information controlled in a fashion equivalent to or greater than Federal employee's access is controlled?	Is vendor/contractor access to information periodically reviewed to ensure that access is controlled in a fashion equivalent to or greater than Federal employee's access is controlled?	Is control of vendor/contractor access to information at a level that is equivalent to or greater than Federal employee's access is controlled standard business practice?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
1.6.17	Computer Security Management and Culture	Personnel Controls	Is access to high-risk program information limited to those with a need for access?	OMB Cir A-130 App III; GISRA	Is there a policy that requires access to high-risk program information be limited to those with a need for access?	Are there procedures for restricting access to high-risk program information to those with a need for access?	Is access to high-risk program information limited to those with a need for access?	Is access to high-risk program information periodically reviewed by an independent third party to ensure access is limited to those with a need for access?	Is restricting access to high-risk program information to those with a need for access standard business practice?
1.6.18	Computer Security Management and Culture	Personnel Controls	Do the job descriptions for positions on high-risk programs accurately reflect the individual's role?	OMB Cir A-130 App III; GISRA	Is there a policy that requires job descriptions for positions on high-risk programs to accurately reflect the individual's role?	Are there procedures for ensuring job descriptions for positions on high-risk programs accurately reflect the individual's role?	Do the job descriptions for positions on high-risk programs accurately reflect the individual's role?	Are job descriptions for positions on high-risk programs periodically reviewed to ensure accurate reflection of the individual's role?	Do job descriptions for positions on high-risk programs accurately reflect the individual's role? Is this standard business practice?
1.7.1	Computer Security Management and Culture	Program Specific Controls	Have specific controls been identified and incorporated in the security configuration based on the specific requirements of the high-risk program?	GISRA	Is there a policy that requires identification and incorporation of program specific controls in the security configuration based on the specific requirements of the high-risk program?	Are there procedures for identification and incorporation of program specific controls in the security configuration based on the specific requirements of the high-risk program?	Have specific controls been identified and incorporated in the security configuration based on the specific requirements of the high-risk program?	Are program specific controls periodically reviewed to ensure they reflect the specific requirements of the high-risk program?	Are the program specific controls in the security configuration based on the specific requirements of the high-risk program? Is this standard business practice?
1.7.2	Computer Security Management and Culture	Program Specific Controls	Are the program specific controls based on commitments to requirements that are outside the specific scope of the established security rules?	GISRA	Is there a policy that requires program specific controls to be based on commitments to requirements that are outside the specific scope of the established security rules?	Are there procedures for implementing program specific controls based on commitments to requirements that are outside the specific scope of the established security rules?	Are the program specific controls based on commitments to requirements that are outside the specific scope of the established security rules?	Are the program specific controls based on commitments to requirements that are outside the specific scope of the established security rules?	Are program specific controls based on commitments to requirements that are outside the specific scope of the established security rules standard business practice?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
2.1.1	Computer Security Plans	System Security Plan	Has each system security plan been updated, reviewed, and approved and otherwise current?	NIST SP 800-18; OMB Cir A-130 App III; FISCAM SP-2.1	Is there a policy that requires the production, update, and review of system security plans on a periodic basis or when a major application or general support system is implemented or significantly changed?	Are there procedures for the production, update, and review of system security plans on a periodic basis or when a major application or general support system is implemented or significantly changed?	Are system security plans developed, updated, and reviewed on a periodic basis or when a major application/general support system is implemented or significantly changed?	Are system security plans examined periodically to ensure the plans reflect the systems at time of examination?	Is up-to-date system security planning an integral part of doing business?
2.1.2	Computer Security Plans	System Security Plan	Is each security plan periodically reviewed and monitored for effectiveness in dealing with threats, vulnerabilities and weaknesses?	OMB Cir A-130 App III; FISCAM SP-2.1; NIST SP 800-18	Is there a policy that requires periodic review of security plans for effectiveness in dealing with threats, vulnerabilities and weaknesses?	Are there procedures for periodic review of security plans for effectiveness in dealing with threats, vulnerabilities and weaknesses?	Are security plans periodically reviewed for effectiveness in dealing with threats, vulnerabilities and weaknesses?	Is there an examination to determine if security plans are periodically reviewed for effectiveness in dealing with threats, vulnerabilities and weaknesses?	Is periodic review of security plans for effectiveness in dealing with threats, vulnerabilities and weaknesses a generally accepted and followed course of action?
2.1.3	Computer Security Plans	System Security Plan	Is a system security plan documented for each system and all interconnected systems?	OMB Cir A-130 App III; FISCAM SP-2.1; NIST SP 800-18; GISRA	Is there a policy requiring a system security plan for all systems and all interconnected systems?	Are there procedures for producing system security plans for all systems and all interconnected systems?	Are there system security plans for systems and interconnected systems?	Is a periodic inspection performed to ensure that current system security plans exist for all systems and interconnected systems?	Is the presence of current system security plans for all systems and interconnected systems considered simply part of doing business?
2.1.4	Computer Security Plans	System Security Plan	Do key affected parties and management approve each system security plan?	FISCAM SP-2.1; NIST SP 800-18; OMB Cir A-130 App III	Is there a policy requiring system security plan approval by key affected parties and management? Does the policy specify who is authorized and required to approve system security plans?	Are there procedures for system security plan approval by key affected parties and management?	Do key affected parties and management approve the system security plan in writing?	Do key affected parties and management approve all system security plans in writing?	Is security plan approval considered simply part of doing business?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
2.1.5	Computer Security Plans	System Security Plan	Does each system security plan contain the topics prescribed in NIST Special Publication 800-18?	NIST SP 800-18; OMB Cir A-130 App III	Is there a policy requiring each system security plan to contain the topics prescribed in NIST Special Publication 800-18?	Are there procedures for incorporating the topics prescribed in NIST Special Publication 800-18 into each system security plan?	Does the security plan makes use of the major guidelines prescribed in NIST Special Publication 800-18, as a minimum base from which to construct the elements of a security plan?	Are security plans examined to ensure that they make use of the major guidelines prescribed in NIST Special Publication 800-18, as a minimum base from which to construct the elements of a security plan?	Do security plans generally and without exception make use of the major guidelines prescribed in NIST Special Publication 800 18, as a minimum base from which to construct the elements of a security plan? Is this considered part of doing business?
2.1.6	Computer Security Plans	System Security Plan	Is a summary of the system security plans incorporated into the strategic Information Resource Management (IRM) plan?	NIST SP 800-18; OMB Cir A-130 App III	Is there a policy requiring that a summary of the system security plan be incorporated within the strategic Information Resource Management -- IRM plan?	Are there procedures for inclusion of a summary of the system security plan within the strategic Information Resource Management -- IRM plan?	Is a summary of the security plan incorporated into the strategic Information Resources Management plan?	Is a copy of the IRM plan reviewed for evidence that it has incorporated a summary of the system security plans?	Does the IRM plan ensure that security objectives are aligned with mission objectives?
2.1.7	Computer Security Plans	System Security Plan	Is each system security plan reviewed periodically and adjusted to reflect current conditions and risks?	NIST SP 800-18; FISCAM SP-2.1; OMB Cir A-130 App III	Is there a policy requiring that major application and general support system security plans be updated at least every three years to reflect current conditions and risks even if there are no changes to the system?	Are there procedures for updating major application and general support system security plans at least every three years to reflect current conditions and risks even if there are no changes to the system?	Are major application and general support system security plans reviewed and updated at least every three years to reflect current conditions and risks even if there are no changes to the system?	Is evidence obtained that each security plan is reviewed and adjusted by a date less than three years ago? Are changes to the prior plan readily identifiable within the current plan?	Are security plans tracked with sufficient lead-time to assign, complete, and approve a new plan before the old plan expires? Is there a sunset date contained within each plan?
2.2.1	Computer Security Plans	Risk Management	Are risk assessments performed and documented on a regular basis (~every 3 years) or whenever the system, facilities, or other conditions change?	FISCAM SP-1; OMB Cir A-130 App III	Is there a policy requiring that risk assessments be performed and documented on a regular basis (~every 3 years) or whenever the system, facilities, or other conditions change?	Are there procedures for performing risk assessments on a regular basis (~every 3 years) or whenever the system, facilities, or other conditions change?	Are risk assessments performed and documented on a regular basis (~every 3 years) or whenever the system, facilities, or other conditions change?	Are risk assessments inspected to ensure that they have been performed and documented on a regular basis (~every 3 years) or whenever the system, facilities, or other conditions change?	Is the risk assessment process integrated into the change control and certification and accreditation process so that systems lacking adequate risk assessments are not placed into production?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
2.2.2	Computer Security Plans	Risk Management	Have threat sources, both natural and manmade, been identified?	FISCAM SP-1; OMB Cir A-130 App III	Is there a policy requiring identification of threat sources, both natural and manmade?	Are there procedures for identification of threat sources, both natural and manmade?	Have threat sources, both natural and manmade, been identified?	Have identified threat sources, both natural and manmade, been verified?	Is threat identification considered part of the risk assessment process?
2.2.3	Computer Security Plans	Risk Management	Has a list of all known system vulnerabilities, system flaws, or weaknesses that could be exploited by the threat sources been developed?	NIST SP 800-26; NIST SP 800-30; OMB Cir A-130 App III	Is there a policy requiring development of a list of all known system vulnerabilities, system flaws, or weaknesses that could be exploited by the threat sources?	Are there procedures for developing a list of all known system vulnerabilities, system flaws, or weaknesses that could be exploited by the threat sources?	Has a list of all known system vulnerabilities, system flaws, or weaknesses that could be exploited by the threat sources been developed?	Has the list of all known system vulnerabilities, system flaws, or weaknesses that could be exploited by the threat sources been verified?	Is the list of all known system vulnerabilities, system flaws, or weaknesses that could be exploited by the threat sources an integral part of all system development and maintenance?
2.2.4	Computer Security Plans	Risk Management	Has an analysis been conducted that determines whether the security requirements in place adequately mitigate vulnerabilities?	NIST SP 800-30; OMB Cir A-130 App III	Is there a policy that requires analysis be conducted of whether the security requirements in place adequately mitigate vulnerabilities?	Are there procedures for performing an analysis of whether the security requirements in place adequately mitigate vulnerabilities?	Has an analysis of whether the security requirements in place adequately mitigate vulnerabilities been performed?	Have the security requirements in place been tested to ensure that they adequately mitigate vulnerabilities? Is the test data used representative of potential vulnerabilities?	Is security requirements examination with respect to vulnerabilities a commonplace occurrence?
2.2.5	Computer Security Plans	Risk Management	Has a consequence assessment, which estimates the degree of harm or loss that could occur as a result of the vulnerabilities, been conducted?	NIST SP 800-30; OMB Cir A-130 App III	Is there a policy requiring that a consequence assessment be conducted?	Are there procedures for conducting a consequence assessment?	Has a consequence assessment been conducted?	Has the consequence assessment been verified by a third party?	Is the consequence assessment an integral part of the system life cycle?
2.2.6	Computer Security Plans	Risk Management	Do program officials understand the risk to systems under their control and determine the acceptable level of risk?	OMB Cir A-130 App III	Is there a policy that requires program officials to understand the risk to systems under their control and determine the acceptable level of risk?	Are there procedures for program officials to gain an understanding of the risk to systems under their control and determine the acceptable level of risk?	Do program officials have an understanding of the risk to systems under their control and determine the acceptable level of risk?	Have program officials understanding of the risk to systems under their control and the determination of the acceptable level of risk been verified?	Do program officials generally understand the risk to systems under their control and do they generally determine the acceptable level of risk?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
2.2.7	Computer Security Plans	Risk Management	Are final risk determinations and related management decisions documented and maintained on file?	FISCAM SP-1; OMB Cir A-130 App III	Is there a policy that requires final risk determinations and related management decisions to be documented and maintained on file?	Are there procedures for documenting and maintaining final risk determinations and related management decisions?	Have final risk determinations and related management decisions been documented and maintained on file?	Is there a periodic review to verify that final risk determinations and related management decisions are documented and maintained on file?	Are documented risk determinations and management approvals for all major applications and general support systems part of the life cycle and are they enforced by the change control process?
2.2.8	Computer Security Plans	Risk Management	Have additional controls been identified and incorporated to sufficiently mitigate identified risks?	NIST SP 800-30; OMB Cir A-130 App III	Is there a policy that requires identification and incorporation of additional controls to sufficiently mitigate identified risks?	Are there procedures for identification and incorporation of additional controls to sufficiently mitigate identified risks?	Have additional controls to sufficiently mitigate identified risks been identified and incorporated?	Have the additional controls to sufficiently mitigate identified risks been tested with appropriate test scenarios?	Are additional controls for mitigating identified risks an integral part of the risk management process?
2.2.9	Computer Security Plans	Risk Management	If automated tools are used, have risk assessment reports been generated?	NIST SP 800-18	Is there a policy that requires generation of risk assessment reports when automated tools are used?	Are there procedures for generation of risk assessment reports when automated tools are used?	Have risk assessment reports been generated when automated tools are used?	Have risk assessment reports been validated by a third party?	Do the risk assessment reports match risk experienced by the agency or similar agencies?
2.2.10	Computer Security Plans	Risk Management	Have specific classes of threats from individual actors, such as those from insiders, hackers, or terrorists, been defined and appropriately considered and used in the risk analysis process?	NIST SP 800-18	Is there a policy that requires specific classes of threats from individual actors, such as those from insiders, hackers, or terrorists, be defined and appropriately considered and used in the risk analysis process?	Are there procedures for identification and incorporation of specific classes of threats from individual actors, such as those from insiders, hackers, or terrorists, in the risk analysis process?	Have specific classes of threats from individual actors, such as those from insiders, hackers, or terrorists, been incorporated into the risk analysis process?	Has the incorporation of specific classes of threats from individual actors, such as those from insiders, hackers, or terrorists, into the risk analysis process been verified by a third party?	Is incorporation of specific classes of threats from individual actors, such as those from insiders, hackers, or terrorists, into the risk analysis process a standard way of doing business?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
2.2.11	Computer Security Plans	Risk Management	Are threats specific to evolving technologies appropriately considered in the risk analysis process (such as those from personal electronic devices -- laptops, palm-sized computers, digital cameras, phones, etc.)?	NIST SP 800-18	Is there a policy that requires threats specific to evolving technologies be appropriately considered in the risk analysis process (such as those from personal electronic devices -- laptops, palm-sized computers, digital cameras, phones, etc.)?	Are there procedures for appropriately considering threats specific to evolving technologies in the risk analysis process (such as those from personal electronic devices -- laptops, palm-sized computers, digital cameras, phones, etc.)?	Have threats specific to evolving technologies been appropriately considered in the risk analysis process (such as those from personal electronic devices -- laptops, palm-sized computers, digital cameras, phones, etc.)?	Has the incorporation of threats specific to evolving technologies into the risk analysis process (such as those from personal electronic devices -- laptops, palm-sized computers, digital cameras, phones, etc.) been verified by a third party?	Is the incorporation of threats specific to evolving technologies into the risk analysis process (such as those from personal electronic devices -- laptops, palm-sized computers, digital cameras, phones, etc.) an integral part of the risk management process?
2.3.1	Computer Security Plans	Authorized Processing	Is certification testing of security controls conducted and documented?	NIST SP 800-18; OMB Cir A-130 App III	Is there a policy that requires certification testing of security controls be conducted and documented?	Are there procedures for conducting and documenting certification testing of security controls?	Is there evidence that procedures for conducting and documenting certification testing of security controls have been implemented? Is the evidence of testing found to be comprehensive?	Has certification testing of security controls been conducted and documented?	Is conducting and documenting certification testing of security controls an integral part of the risk management process?
2.3.2	Computer Security Plans	Authorized Processing	Has each application undergone a technical evaluation within the past 3 years or when a significant change occurred to ensure that it meets applicable federal laws, regulations, policies, guidelines, and standards?	OMB Cir A-130 App III; NIST SP 800-18; GISRA	Is there a policy that requires each application undergo a technical evaluation at least every 3 years or when a significant change occurs to ensure that it meets applicable federal laws, regulations, policies, guidelines, and standards?	Are there procedures for conducting a technical evaluation of an application at least every 3 years or when a significant change occurs to ensure that it meets applicable federal laws, regulations, policies, guidelines, and standards?	Have technical evaluations of each application been conducted at least every 3 years or when a significant change occurs to ensure that it meets applicable federal laws, regulations, policies, guidelines, and standards?	Have the technical evaluations of each application been reviewed to ensure that an appropriate evaluation has been conducted on the appropriate schedule?	Is the technical application evaluation integrated with the accreditation and evaluation process, the life-cycle process, and the change controls process?
2.3.3	Computer Security Plans	Authorized Processing	Does each system have written authorization to operate either on an interim basis with planned corrective action or full authorization?	OMB Cir A-130 App III; NIST SP 800-18	Is there a policy that requires each system to have written authorization to operate either on an interim basis with planned corrective action or full authorization?	Are there procedures for obtaining written authorization to operate either on an interim basis with planned corrective action or full authorization?	Does each system have written authorization to operate either on an interim basis with planned corrective action or full authorization?	Has each system authorization to operate either on an interim basis with planned corrective action or full authorization been verified?	Is system authorization to operate either on an interim basis with planned corrective action or full authorization been verified an accepted way of doing business?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
2.3.4	Computer Security Plans	Authorized Processing	Has each system been certified/re-certified and authorized to process information (accreditation)?	OMB Cir A-130 App III; NIST SP 800-18	Is there a policy that requires each system to be certified/re-certified and authorized to process information (accreditation)?	Are there procedures for certifying/re-certifying systems and authorizing to process information (accreditation)?	Has each system been certified/re-certified and authorized to process information (accreditation)?	Has each system certification/re-certification and authorization to process information (accreditation) been verified by a third party?	Is system certification/re-certification and authorization to process information (accreditation) an integral part of doing business?
2.3.5	Computer Security Plans	Authorized Processing	Are in-place safeguards operating as intended?	OMB Cir A-130 App III; NIST SP 800-18	Is there a policy that requires in-place safeguards to operate as intended?	Are there procedures for ensuring that in-place safeguards operate as intended?	Do in-place safeguards operate as intended?	Are in-place safeguards tested to verify operation as intended?	Is an effort made to provide formal methods assurance that existing controls are operating as intended?
2.3.6	Computer Security Plans	Authorized Processing	Is any system operating on an interim authority to process?	OMB Cir A-130 App III; NIST SP 800-18	Is there a policy that allows systems to operate on an interim authority to process? Is there a time limit?	Are there procedures for providing systems an interim authority to process? Is there a procedure outlining how to transition to full authority to process?	Are all systems operating on an interim authority to process in full compliance with the policies and procedures?	Is there a frequent review of all systems operating on an interim authority to process to ensure this is still an acceptable state?	Is there full justification for systems that operate on an interim authority to process? Is this justification an integral part of the operating environment?
2.3.7	Computer Security Plans	Authorized Processing	Are there certification and accreditation documents and a statement authorizing each system to process including the acceptance of residual risk?	NIST SP 800-18	Is there a policy that requires certification and accreditation documents and a statement authorizing each system to process including the acceptance of residual risk?	Are there procedures for developing certification and accreditation documents and obtaining a statement authorizing each system to process including the acceptance of residual risk?	Are there certification and accreditation documents and a statement authorizing the system to process for each system including the acceptance of residual risk?	Is each system periodically reviewed to verify the certification and accreditation documentation for each system including the acceptance of residual risk?	Is it generally accepted practice to have current, appropriate certification and accreditation documentation and a statement authorizing each system to process including the acceptance of residual risk?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
2.3.8	Computer Security Plans	Authorized Processing	Have interconnection agreements or similar documents been defined at the system, enterprise or at the macro level to specify how information is exchanged, and the security measures to ensure the integrity of a trusted relationship?	OMB Cir A-130 App III	Is there a policy that requires interconnection agreements or similar documents to be defined at the system, enterprise or at the macro level to specify how information is exchanged, and the security measures to ensure the integrity of a trusted relationship?	Are there procedures for development of interconnection agreements or similar documents to be defined at the system, enterprise or at the macro level to specify how information is exchanged, and the security measures to ensure the integrity of a trusted relationship?	Are there interconnection agreements or similar documents to be defined at the system, enterprise or at the macro level to specify how information is exchanged, and the security measures to ensure the integrity of a trusted relationship?	Are the interconnection agreements or similar documents (defined at the system, enterprise or at the macro level) that specify how information is exchanged, and the security measures to ensure the integrity of a trusted relationship periodically reviewed to ensure current information?	Is it general business practice to have current interconnection agreements or similar documents (defined at the system, enterprise or at the macro level) that specify how information is exchanged, and the security measures to ensure the integrity of a trusted relationship?
2.3.9	Computer Security Plans	Authorized Processing	Have interconnection agreements or similar documents been factored into the acceptance of risk?	OMB Cir A-130 App III	Is there a policy that requires interconnection agreements or similar documents to be factored into the acceptance of risk?	Are there procedures for incorporating interconnection agreements or similar documents into the acceptance of risk?	Are interconnection agreements or similar documents factored into the acceptance of risk?	Has the incorporation of interconnection agreements or similar documents into the acceptance of risk been reviewed by a third party?	Is the incorporation of interconnection agreements or similar documents into the acceptance of risk a basic business practice?
2.4.1	Computer Security Plans	Documentation	Are the current system configurations documented, including links to other systems?	OMB Cir A-130 App III; NIST SP 800-18	Is there a policy that requires documentation of current system configurations, including links to other systems?	Are there procedures for documentation of current system configurations, including links to other systems?	Are the current system configurations documented, including links to other systems?	Have the current system configurations been reviewed against the documentation, including links to other systems?	Are current system configurations incorporated into system documentation and part of the basic way of doing business?
2.4.2	Computer Security Plans	Documentation	Is vendor-supplied documentation of purchased software available to users?	NIST SP 800-18	Is there a policy that requires availability of vendor-supplied documentation of purchased software?	Are there procedures for making vendor-supplied documentation of purchased software available to users?	Is vendor-supplied documentation of purchased software available to users?	Is available vendor-supplied documentation of purchased software periodically reviewed to ensure all software has available documentation?	Is it generally accepted practice to ensure that vendor-supplied documentation of purchased software is available to users?
2.4.3	Computer Security Plans	Documentation	Is there vendor-supplied documentation of purchased hardware?	NIST SP 800-18	Is there a policy that requires availability of vendor-supplied documentation of purchased hardware?	Are there procedures for making vendor-supplied documentation of purchased hardware available to users?	Is vendor-supplied documentation of purchased hardware available to users?	Is available vendor-supplied documentation of purchased hardware periodically reviewed to ensure all hardware has available documentation?	Is it generally accepted practice to ensure that vendor-supplied documentation of purchased hardware is available to users?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
2.4.4	Computer Security Plans	Documentation	Is there application documentation for custom applications?	NIST SP 800-18	Is there a policy that requires availability of documentation of custom applications?	Are there procedures for making documentation of custom applications available to users?	Is documentation of custom applications available to users?	Is available documentation of custom applications periodically reviewed to ensure all software has available documentation?	Is it generally accepted practice to ensure that documentation of custom applications is available to users?
2.4.5	Computer Security Plans	Documentation	Are there current network diagrams and documentation on setups of routers and switches?	NIST SP 800-18	Is there a policy that requires current network diagrams and documentation on setups of routers and switches?	Are there procedures for development of network diagrams and documentation on setups of routers and switches?	Are there current network diagrams and documentation on setups of routers and switches?	Are the network diagrams and documentation on setups of routers and switches periodically reviewed to ensure they are current?	Are current network diagrams and documentation on setups of routers and switches a standard way of doing business?
3.1.1	Security Awareness, Training, and Education	End users' security awareness and training	Have employees and contractors received adequate training to fulfill their security responsibilities prior to access to the system?	NIST SP 800-16; OMB Cir A-130 App III	Is there a current complete, quality policy addressing employee and contractor security awareness and training?	Are there complete and current procedures that address training for employees and contractors? Has accountability been established to implement the procedures?	Have employees and contractors been trained at a sufficient frequency and to a sufficient level of detail? Do employees and contractors have a complete understanding of their IT security responsibilities?	Is there a periodic assessment of employees and contractors understanding of their IT security responsibilities?	Is IT security an integral part of the duties of employees and contractors?
3.1.2	Security Awareness, Training, and Education	End users' security awareness and training	Is employee IT security training and professional development documented and monitored?	FISCAM SP-4.2; GISRA	Is there a current complete, quality policy addressing employee security training and professional development?	Are there current procedures for employee IT security training and professional development?	Have employees received IT security training and professional development on a periodic basis?	Is employee's IT security knowledge periodically evaluated?	Is employee IT security training and professional development an integral part of doing business?
3.1.3	Security Awareness, Training, and Education	End users' security awareness and training	Is IT security training based on established training requirements?	GISRA	Is there a policy that specifies IT security training requirements? Is a security awareness program required?	Are there procedures for initial security training? Are there procedures for periodic security retraining? Are there procedures the IT security training requirements?	Have all employees gone through initial security training? Have all employees been periodically retrained according to the policy? Have all employees received the IT security training spelled out in the requirements?	Is the extent of security training assessed against the security requirements on a periodic basis?	Are the security requirements an integral part of the organizations overall IT Security Program?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
3.1.4	Security Awareness, Training, and Education	End users' security awareness and training	Are IT security training requirements and responsibilities identified in the system acquisition documents?	GISRA	Is there a policy for specification of IT security training requirements and responsibilities in system acquisitions documents?	Are there procedures for including IT security training requirements within the IT system acquisition materials?	Are IT security training requirements and responsibilities identified in the system acquisition documents?	Are system acquisition documents reviewed to ensure incorporation of IT security training requirements prior to release?	Is it generally accepted that IT security training requirements must be present in system acquisition documents? Is it part of the way of doing business?
3.1.5	Security Awareness, Training, and Education	End users' security awareness and training	Do IT security trainers have sufficient knowledge of computer security issues, principles and techniques?	GISRA	Is there a policy specifying that trainers must have sufficient knowledge of computer security issues, principles and techniques?	Is there a procedure for evaluating IT security trainers?	Are IT security trainers evaluated?	Is there follow-up to ensure that the IT security trainer evaluation process works?	Are IT security trainers almost always knowledgeable about current computer security issues, principles and techniques?
3.1.6	Security Awareness, Training, and Education	End users' security awareness and training	Are users trained on basic system access rules and ethical uses systems?	GISRA	Is there a policy requiring users to be trained on basic system access rules and ethical uses of systems? Do training requirements identify the basic end user system access rules and guidance on ethical use?	Are there procedures for training users on basic system access rules and ethical uses of systems?	Are all users are trained on basic system access rules and ethical uses of the system?	Is user's knowledge of basic system access rules and ethics evaluated?	Is user's knowledge of basic system access rules and ethics high, commonplace, and accepted as a way of doing business?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
3.1.7	Security Awareness, Training, and Education	End users' security awareness and training	Is mandatory annual refresher IT security training for employees and contractors conducted? Is this training based on the sensitivity of the information the employee or contractor handles?	OMB Cir A-130 App III; NIST SP 800-16	Is there a policy that specifies mandatory annual refresher IT security training that is based upon the sensitivity of information the employee or contractor handles?	Are there procedures for providing employees and contractors appropriate IT security training?	Is refresher training scheduled on a periodic basis, and evidenced by attendance rosters?	Is the IT security knowledge of employees and contractors assessed?	Is refresher training integrated into the overall IT Security Program and updated with relevant information?
3.1.8	Security Awareness, Training, and Education	End users' security awareness and training	Are methods employed to make employees aware of security, i.e., posters, booklets?	NIST SP 800-18	Is there a policy that specifies a requirement to make employees aware of security?	Are there documented procedural requirements for conducting a security awareness program to make employees aware of IT security issues?	Are standard methodologies and procedures employed to make employees aware of agency security? Is Awareness program verified through observation?	Is employee's awareness of IT security periodically assessed?	Are awareness issues current and updated from recent CSIRC/FedCIRC data? Are the methods used to make employees aware of security effective and refreshed periodically?
3.1.9	Security Awareness, Training, and Education	End users' security awareness and training	Have employees received a copy of or have easy access to agency security procedures and policies?	NIST SP 800-18	Is there a policy for making agency security procedures easily accessible by all employees?	Are there procedures specifying mechanisms for dissemination of organizational and system level security policies and procedures?	Do all employees have easy access to agency security procedures and policies?	Have employees been queried regarding the ease of access?	Do all employees have easy access to all agency security procedures and policies and are all readily aware of and able to obtain them?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
3.1.10	Security Awareness, Training, and Education	End users' security awareness and training	Are personnel trained to recognize and handle incidents?	NIST SP 800-18; FISCAM SP-3.4	Is there a policy regarding employee training for incident response?	Are there procedures for training personnel on how to recognize and handle incidents?	Are personnel trained on how to recognize and handle incidents?	Are staff skills in recognizing and handling incidents periodically assessed?	Do all employees understand how to recognize and handle current incidents?
3.1.11	Security Awareness, Training, and Education	End users' security awareness and training	Have new employees received security training within 60 days of hire?	NIST SP 800-16	Is there a policy requiring that new employees receive security training within 60 days of hire?	Are there procedures for providing new employees with current security training within 60 days of hire?	Are new employees provided with IT security training within 60 days of hire?	Are new employees IT security knowledge evaluated after training?	Are all new employees knowledgeable of IT security within 60 days of hire?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
3.1.12	Security Awareness, Training, and Education	End users' security awareness and training	Do employees receive additional IT security training whenever there is a significant change in the agency's IT security environment?	NIST SP 800-16	Is there a policy requiring employees to receive additional IT security training whenever there is a significant change in the agency's IT security environment?	Are there procedures for providing employees with additional IT security training whenever there is a significant change in the agency's IT security environment?	Do employees receive additional IT security training whenever there is a significant change in the agency's IT security environment?	Is employee's knowledge periodically assessed after receiving additional IT security training whenever there is a significant change in the agency's IT security environment?	Is additional IT security training for all employees whenever there is a significant change in the agency's IT security environment part of doing business?
3.1.13	Security Awareness, Training, and Education	End users' security awareness and training	Do employees receive additional security training if they enter a new position that has different IT security requirements?	NIST SP 800-16	Is there policy requiring additional security training when employees enter a new position that has different IT security requirements?	Are there procedures for additional security training if employees enter a new position that has different IT security requirements?	Do employees receive additional security training when they enter a new position that has different IT security requirements?	Is employee's IT security knowledge assessed after they receive additional security training when they enter a new position that has different IT security requirements?	Do all employees receive additional security training if they enter a new position that has different IT security requirements? Is this generally accepted as the way of doing business?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
3.1.14	Security Awareness, Training, and Education	End users' security awareness and training	Are employees aware of and trained on the system's rules of behavior? Are the system rules of behavior documented?	OMB Cir A-130 App III	Is there a policy requiring employees to be aware of and trained on the system's rules of behavior?	Are there procedures for employees to be made aware of and trained on the system's rules of behavior?	Are employees made aware of and trained on the system's rules of behavior?	Is employee's knowledge of the system's rules of behavior periodically assessed?	Are all employees knowledgeable of the system's rules of behavior? Is this knowledge considered second nature?
3.2.1	Security Awareness, Training, and Education	IT professionals' security awareness and training	Is specialized IT security training based on the functional responsibilities of the user?	GISRA	Is there a policy for specialized training based on the functional responsibilities of the user?	Are there procedures for providing specialized training based on the functional responsibilities of the user?	Do employees receive specialized training based on their functional responsibilities?	Is each employee's knowledge of the specialized training periodically assessed?	Is specialized training an integral part of an employee's job?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
3.2.2	Security Awareness, Training, and Education	IT professionals' security awareness and training	Are IT personnel required to have periodic refresher training related to current IT security vulnerabilities?	GISRA	Is there a policy requiring periodic IT security fresher training for IT professionals? Is the periodicity frequent enough?	Are there procedures for providing periodic IT security fresher training for IT professionals?	Do IT professionals receive periodic IT security fresher training for IT professionals? Is this training received on a frequent enough basis?	Have the IT professionals knowledge of IT security been assessed relative to the areas of responsibility?	Is periodic IT security fresher training for IT professionals an integral part of each employees job?
3.3.1	Security Awareness, Training, and Education	Management security awareness and training	Is management conscious of computer security requirements required to effectively meet mission requirements?	GISRA; OMB Cir A-130 App III	Is there a policy requiring management to be aware of IT security requirements?	Are there procedures for making management aware of IT security requirements?	Is management made aware of current IT security requirements?	Is management knowledge of current IT security requirements periodically assessed?	Is management an integral part of the IT security knowledge base?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
3.3.2	Security Awareness, Training, and Education	Management security awareness and training	Are metrics used to improve the enterprise computer security training and awareness program?	GISRA	Is there a policy that requires use of metrics to improve the enterprise computer security training and awareness program?	Are there procedures for the using metrics to improve the computer security training and awareness program?	Are metrics used to improve the enterprise computer security training and awareness program?	Are the metrics used to improve the enterprise computer security training and awareness program periodically reviewed to ensure effectiveness?	Is using metrics to improve the computer security training and awareness program standard business practice?
3.3.3	Security Awareness, Training, and Education	Management security awareness and training	Are computer security metrics used to track the computer security training and awareness program performance, assess the costs and benefits of security training and awareness, and provide feedback to management?	GISRA	Is there a policy that requires computer security training and awareness metrics be used to track computer security training and awareness program performance, assess the costs and benefits of security training and awareness, and provide feedback to management?	Are there procedures for use of computer security training and awareness metrics to track computer security program performance, assess the costs and benefits of computer security training and awareness, and provide feedback to management?	Are computer security metrics used to track computer security training and awareness program performance, assess the costs and benefits of computer security training and awareness, and provide feedback to management?	Are computer security training and awareness metrics that track computer security program performance, assess the costs and benefits of computer security training and awareness, and provide feedback to management periodically reviewed to ensure effectiveness?	Are computer security training and awareness metrics that track computer security program performance, assess the costs and benefits of computer security training and awareness, and provide feedback to management part of the standard business practice?
3.3.4	Security Awareness, Training, and Education	Management security awareness and training	Does management understand and use the security training and awareness metrics information?	Best Engineering Practice	Is there a policy that requires management to understand and use the security training and awareness metrics information?	Are there procedures for management to understand and use the security training and awareness metrics information?	Does management understand and use the security training and awareness metrics information?	Is management understand and use the security training and awareness metrics information periodically evaluated to ensure effectiveness?	Is management understanding and use of security training and awareness metrics information standard business practice?
3.3.5	Security Awareness, Training, and Education	Management security awareness and training	Do incentives from management function to encourage security training and awareness?	GISRA	Is there a policy that requires incentives to encourage security training and awareness?	Are there procedures for developing and using incentives to encourage security training and awareness?	Do incentives from management function to encourage security training and awareness?	Are incentives from management to encourage security training and awareness periodically evaluated for effectiveness?	Is the use of incentives to encourage security training and awareness standard business practice?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
3.3.6	Security Awareness, Training, and Education	Management security awareness and training	Is computer security training and awareness used to evaluate employee performance?	GISRA	Is there a policy that requires computer security training and awareness be used to evaluate employee performance?	Are there procedures for using computer security training and awareness to evaluate employee performance?	Is computer security training and awareness used to evaluate employee performance?	Is the effectiveness of using computer security training and awareness to evaluate employee performance periodically reviewed for effectiveness?	Is the use of computer security training and awareness to evaluate employee performance standard business practice?
3.4.1	Security Awareness, Training, and Education	Program Specific Security Training	Do IT developers and maintenance personnel understand program specific IT security requirements?	GISRA	Is there a policy requiring IT developers and maintainers to have knowledge of program specific IT security requirements?	Are there procedures for training IT developers and maintenance personnel on program specific IT security requirements?	Are IT developers and maintenance personnel trained on program specific IT security requirements?	Are IT developers and maintenance personnel knowledgeable of program specific IT security requirements? Is their knowledge level periodically assessed?	Are IT developers and maintenance personnel knowledgeable of how security awareness training is an integral part of the program?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
3.4.2	Security Awareness, Training, and Education	Program Specific Security Training	Do program users understand program specific IT security requirements?	GISRA	Is there policy requiring program users to have knowledge of program specific IT security requirements?	Are there procedures for training program users on program specific IT security requirements?	Are program users trained on program specific IT security requirements?	Is program user's knowledge of program specific IT security requirements periodically assessed?	Are IT users knowledgeable of how security awareness training is an integral part of the program?
3.4.3	Security Awareness, Training, and Education	Program Specific Security Training	Do program managers understand program specific IT security requirements?	GISRA	Is there policy requiring program managers to have knowledge of program specific IT security requirements?	Are there procedures for training program managers on program specific IT security requirements?	Are program managers trained on program specific IT security requirements?	Are program managers knowledge of program specific IT security requirements periodically assessed?	Are program managers knowledgeable of how security awareness training is an integral part of the program?
4.1.1	Budget and Resources	IT security part of capital planning process	Has a mission/business impact analysis been conducted within the past year from an information security perspective?	NIST SP 800-30; OMB Cir A-130 App III	Is there a policy that requires a mission/business impact analysis be conducted within the past year from an information security perspective?	Are there procedures for conducting a mission/business impact analysis from an information security perspective?	Has a mission/business impact analysis been conducted within the past year from an information security perspective?	Is there a periodic review to verify that an effective mission/business impact analysis been conducted within the past year from an information security perspective?	Is conducting a mission/business impact analysis from an information security perspective on a yearly basis standard business practice?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
4.1.2	Budget and Resources	IT security part of capital planning process	Does the business case document the resources required for adequately securing all systems and programs?	Clinger Cohen; GISRA	Is there a policy that requires the business case to document the resources required for adequately securing all systems and programs?	Are there procedures for documenting the resources required for adequately securing all systems and programs in the business case?	Does the business case document the resources required for adequately securing all systems and programs?	Is the business case periodically reviewed to ensure that the resources required for adequately securing all systems and programs is documented?	Is documenting the resources required for adequately securing all systems and programs in the business case standard business practice?
4.1.3	Budget and Resources	IT security part of capital planning process	Does the Investment Review Board ensure any investment request includes the security resources needed?	Clinger Cohen	Is there a policy that requires the Investment Review Board to ensure any investment request includes the security resources needed?	Are there procedures for the Investment Review Board to ensure any investment request includes the security resources needed?	Does the Investment Review Board ensure any investment request includes the security resources needed?	Are the Investment Review Board's investment requests periodically reviewed to ensure that security resources needed are specified?	Is it standard business practice for the Investment Review Board to ensure any investment request includes the security resources needed?
4.1.4	Budget and Resources	IT security part of capital planning process	Does the budget request include the security resources required for the system/program?	GISRA	Is there a policy that requires the budget request include the security resources required for the system/program?	Are there procedures for including the security resources required for the system/program in the budget request?	Does the budget request include the security resources required for the system/program?	Are the budget requests periodically reviewed to ensure inclusion of the security resources required for the system/program?	Is it standard business practice for the budget request to include the security resources required for the system/program?
4.1.5	Budget and Resources	IT security part of capital planning process	In your future capital planning using Exhibit 300B's, have assets or projects reviewed as part of the GISRA report had any weaknesses identified, and if so, have the weaknesses been incorporated into you corrective action plans and funded appropriately?	OMB Cir. A-11, GISRA	Is there a policy requiring that Exhibit 300B's used in future capital planning, that have assets or projects reviewed as part of the GISRA report had any weaknesses identified and the weaknesses incorporated into you corrective action plans and funded appropriately?	Do your procedures require that FY04 Exhibit 300B's that have assets or projects reviewed as part of the GISRA report and had weaknesses identified, been incorporated into you corrective action plans and funded appropriately?	Do your Exhibit 300B's that have assets or projects reviewed as part of the GISRA report and had weaknesses identified, been incorporated into you corrective action plans and funded appropriately?	Are Exhibits 53's reviewed and updated to ensure that the GISRA report and had weaknesses identified, been incorporated into you corrective action plans and funded appropriately?	Is it a standard business practice that Exhibits 53's are related to weaknesses and corrective actions in the GISRA report and that actions are funded appropriately?
4.1.6	Budget and Resources	IT security part of capital planning process	Do your Exhibit 300B identify if the asset/project meets security and privacy requirements?	OMB Cir. A-11	Is there a policy that Exhibit 300B identify if the asset/project meets security and privacy requirements?	Do your procedures require that Exhibit 300B identify if the asset/project meets security and privacy requirements?	Do your Exhibit 300B identify if the asset/project meets security and privacy requirements?	Are Exhibits 53's reviewed and updated to ensure that 300B identify if the asset/project meets security and privacy requirements?	Is it a standard business practice to ensure that Exhibits 53's and 300Bs identify that the asset/project meets security and privacy requirements?
4.1.7	Budget and Resources	IT security part of capital planning process	How does the agency integrate computer security and critical infrastructure protection into capital planning and investment control and were these costs identified in future capital asset plan (and exhibit 53)?	OMB Cir. A-11	Is there a policy that requires the agency to integrate computer security and critical infrastructure protection into capital planning and investment control (were these costs identified in future capital asset plan and exhibit 53)?	Do the procedures require that the agency to integrate computer security and critical infrastructure protection into capital planning and investment control (were these costs identified in future capital asset plan and Exhibit 53)?	Does the agency integrate computer security and critical infrastructure protection into capital planning and investment control (these costs are identified in future capital asset plan and Exhibit 53)?	Are Exhibits 53's? as an output of the capital planning process, reviewed and updated to ensure that computer security and critical infrastructure protection are integrated into capital planning?	Is it a standard business practice that computer security and critical infrastructure protection are integrated into capital planning?
4.1.8	Budget and Resources	IT security part of capital planning process	Do your Exhibit 300B's show CIP costs as line items and will your agency's culture allow for seamless integration?	OMB Cir. A-11	Is there a policy that requires the Exhibit 300B's to show CIP costs as line items?	Do procedures require that Exhibit 300B's show CIP costs as line items?	Do the Exhibit 300B's show CIP costs as a line item and will your agency's culture allow for seamless integration?	Are Exhibits 300B's reviewed and updated to show CIP costs as a line item?	Is it a standard business practice that 300B's show CIP costs as a line item?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
4.1.9	Budget and Resources	IT security part of capital planning process	Are critical infrastructure protection costs included in the breakdown of security costs by each major program office or operating unit?	OMB Cir. A-11	Is there a policy that critical infrastructure protection costs are included the breakdown of security costs by each major program office or operating unit?	Are there procedures for costing critical infrastructure protection that include the breakdown of security costs by each major program office or operating unit?	Do budget documents for each major operating program office or operating unit include Exhibit 300s and Form 53, as applicable, contain this CIP budget information?	Are Exhibits 300B's reviewed and updated when costing critical infrastructure protection to include the breakdown of security costs by each major operating program office or operating unit?	Is it a standard business practice that when costing critical infrastructure protection, that the breakdown of security costs by each major program office or operating unit is included?
4.2.1	Budget and Resources	Adequate resources applied to IT security	Are computer security resources (internal FTEs and funding) adequate to protect information in accordance with assessed risks?	GISRA	Is there a policy that requires allocation of adequate computer security resources (internal FTEs and funding) to protect information in accordance with assessed risks?	Are there procedures for allocation of adequate computer security resources (internal FTEs and funding) to protect information in accordance with assessed risks?	Are computer security resources (internal FTEs and funding) adequate to protect information in accordance with assessed risks?	Are periodic third party examinations conducted to ensure computer security resources (internal FTEs and funding) adequate to protect information in accordance with assessed risks?	Is adequate allocation of computer security resources (internal FTEs and funding) to protect information in accordance with assessed risks standard business practice?
4.3.1	Budget and Resources	IT security funding and resources distributed based upon a risk model	Is the distribution of resources (internal FTEs and funding) based on the assessed risks?	GISRA	Is there a policy that requires distribution of resources (internal FTEs and funding) based on the assessed risks?	Are there procedures for distribution of resources (internal FTEs and funding) based on the assessed risks?	Is the distribution of resources (internal FTEs and funding) based on the assessed risks?	Are periodic third party examinations conducted to ensure the distribution of resources (internal FTEs and funding) is based on the assessed risks?	Is distributing resources (internal FTEs and funding) based on the assessed risks standard business practice?
4.4.1	Budget and Resources	Cost effective IT security solutions	Is resource allocation based on a systematic, risk-based prioritization of issues to ensure cost-effectiveness?	GISRA	Is there a policy that requires resource allocation to be based on a systematic, risk-based prioritization of issues to ensure cost-effectiveness?	Are there procedures for allocating resources based on a systematic, risk-based prioritization of issues to ensure cost-effectiveness?	Is resource allocation based on a systematic, risk-based prioritization of issues to ensure cost-effectiveness?	Are periodic third party examinations conducted to ensure resource allocation is based on a systematic, risk-based prioritization of issues to ensure cost-effectiveness?	Is resource allocation based on a systematic, risk-based prioritization of issues to ensure cost-effectiveness standard business practice?
4.4.2	Budget and Resources	Cost effective IT security solutions	Are risk analyses and return on investment used to determine which security controls should be funded and implemented?	OMB Cir A-130 App III; GISRA	Is there a policy that requires use of risk analyses and return on investment to determine which security controls should be funded and implemented?	Are there procedures for using risk analyses and return on investment to determine which security controls should be funded and implemented?	Are risk analyses and return on investment used to determine which security controls should be funded and implemented?	Are periodic third party examinations conducted to verify that risk analyses and return on investment were used to determine which security controls should be funded and implemented?	Is it standard business practice to use risk analyses and return on investment to determine which security controls should be funded and implemented?
4.4.3	Budget and Resources	Cost effective IT security solutions	Has a cost-benefit analysis been performed within the past year that takes into account financial indicators, stakeholders perception of performance, internal processes, growth, innovation, level of risk, and improvement?	Best practice	Is there a policy that requires performance of a cost-benefit analysis within the past year that takes into account financial indicators, stakeholders perception of performance, internal processes, growth, innovation, level of risk, and improvement?	Are there procedures for performing a cost-benefit analysis that takes into account financial indicators, stakeholders perception of performance, internal processes, growth, innovation, level of risk, and improvement?	Has a cost-benefit analysis been performed within the past year that takes into account financial indicators, stakeholders perception of performance, internal processes, growth, innovation, level of risk, and improvement?	Are periodic third party examinations conducted to verify that a cost-benefit analysis has been performed within the past year that takes into account financial indicators, stakeholders perception of performance, internal processes, growth, innovation, level of risk, and improvement?	Is it standard business practice to perform a yearly cost-benefit analysis that takes into account financial indicators, stakeholders perception of performance, internal processes, growth, innovation, level of risk, and improvement?
4.4.4	Budget and Resources	Cost effective IT security solutions	Are IT security expenditures linked to the strategy and mission of the organization/program?	Best practice	Is there a policy that requires IT security expenditures be linked to the strategy and mission of the organization/program?	Are there procedures for linking IT security expenditures to the strategy and mission of the organization/program?	Are IT security expenditures linked to the strategy and mission of the organization/program?	Are periodic third party examinations conducted to verify that IT security expenditures linked to the strategy and mission of the organization/program?	Is it standard business practice to link IT security expenditures to the strategy and mission of the organization/program?
4.4.5	Budget and Resources	Cost effective IT security solutions	Has funding for capital projects been linked to strategic agency objectives?	Best practice	Is there a policy that requires linking funding for capital projects to strategic agency objectives?	Are there procedures for linking funding for capital projects to strategic agency objectives?	Has funding for capital projects been linked to strategic agency objectives?	Are periodic third party examinations conducted to verify that funding for capital projects has been linked to strategic agency objectives?	Is it standard business practice to link funding for capital projects to strategic agency objectives?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
4.4.6	Budget and Resources	Cost effective IT security solutions	Do your Exhibit 300B's identify the level of security risk and the factor (confidentiality, integrity, or availability) that determines the risk level	OMB Cir. A-11	Is there a policy that requires Exhibit 300B's to identify the level of security risk and the factor (confidentiality, integrity, or availability) that determines the risk level?	Do procedures require that Exhibit 300B's to identify the level of security risk and the factor (confidentiality, integrity, or availability) that determines the risk level?	Do the Exhibit 300B's identify the level of security risk and the factor (confidentiality, integrity, or availability) that determines the risk level?	Do the Exhibit 300B's identify the level of security risk and the factor (confidentiality, integrity, or availability) that determines the risk level?	Is it a standard business practice that Exhibit 300B's identify the level of security risk and the factor (confidentiality, integrity, or availability) that determines the risk level?
4.5.1	Budget and Resources	Procurement Controls	Have contractual requirements from the FAR been included in procurement documents such as the proposal or technical specification for computer security/operations services or products?	FAR; GISRA	Is there a policy that requires contractual requirements from the FAR to be included in procurement documents such as the proposal or technical specification for computer security/operations services or products?	Are there procedures for including contractual requirements from the FAR in procurement documents such as the proposal or technical specification for computer security/operations services or products?	Have contractual requirements from the FAR been included in procurement documents such as the proposal or technical specification for computer security/operations services or products?	Are periodic third party examinations conducted to verify that contractual requirements from the FAR have been included in procurement documents such as the proposal or technical specification for computer security/operations services or products?	Is the inclusion of contractual requirements from the FAR in procurement documents such as the proposal or technical specification for computer security/operations services or products standard business practice?
4.5.3	Budget and Resources	Procurement Controls	Are appropriate security requirements specified in all Statements of Work?	FAR; GISRA	Is there a policy that requires appropriate security requirements to be specified in all Statements of Work?	Are there procedures for specifying appropriate security requirements in all Statements of Work?	Are appropriate security requirements specified in all Statements of Work?	Are periodic third party examinations conducted to verify that appropriate security requirements are specified in all Statements of Work?	Is it standard business practice to specify appropriate security requirements in all Statements of Work?
4.5.4	Budget and Resources	Procurement Controls	Have contractual requirements for position risk level determination been included in contract clauses for computer security operations services?	FAR; GISRA	Is there a policy that requires contractual requirements for position risk level determination to be included in contract clauses for computer security operations services?	Are there procedures for including contractual requirements for position risk level determination in contract clauses for computer security operations services?	Have contractual requirements for position risk level determination been included in contract clauses for computer security operations services?	Are periodic third party examinations conducted to verify that contractual requirements for position risk level determination have been included in contract clauses for computer security operations services?	Is it standard business practice to include contractual requirements for position risk level determination in contract clauses for computer security operations services?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
4.5.5	Budget and Resources	Procurement Controls	Do contract requirements specify physical security reviews of contractor facilities of an off site contractor?	FAR; GISRA	Is there a policy that requires contract requirements to specify physical security reviews of contractor facilities of an off site contractor?	Are there procedures for specifying contract requirements for physical security reviews of contractor facilities of an off site contractor?	Do contract requirements specify physical security reviews of contractor facilities of an off site contractor?	Are periodic third party examinations conducted to verify that contract requirements specify physical security reviews of contractor facilities of an off site contractor?	Is it standard business practice for contract requirements to specify physical security reviews of contractor facilities of an off site contractor?
4.5.6	Budget and Resources	Procurement Controls	Do contract requirements specify requisite contractor personnel security training?	FAR; GISRA	Is there a policy that requires contract requirements to specify requisite contractor personnel security training?	Are there procedures for specifying contract requirements for requisite contractor personnel security training?	Do contract requirements specify requisite contractor personnel security training?	Are periodic third party examinations conducted to verify that contract requirements specify requisite contractor personnel security training?	Is it standard business practice for contract requirements to specify requisite contractor personnel security training?
4.5.7	Budget and Resources	Procurement Controls	Do contract requirements specify restrictions on access to privileged information?	FAR; GISRA	Is there a policy that requires contract requirements to specify restrictions on access to privileged information?	Are there procedures for specifying contract requirements for restrictions on access to privileged information?	Do contract requirements specify restrictions on access to privileged information?	Are periodic third party examinations conducted to verify that contract requirements specify restrictions on access to privileged information?	Is it standard business practice for contract requirements to specify restrictions on access to privileged information?
4.5.8	Budget and Resources	Procurement Controls	Have security relevant contractual requirements including the FAR been included in supplier's contracts for computer security/operations services or products?	FAR; GISRA	Is there a policy that requires security relevant contractual requirements including the FAR be included in supplier's contracts for computer security/operations services or products?	Are there procedures for including security relevant contractual requirements including the FAR in supplier's contracts for computer security/operations services or products?	Have security relevant contractual requirements including the FAR been included in supplier's contracts for computer security/operations services or products?	Are periodic third party examinations conducted to verify that security relevant contractual requirements including the FAR are included in supplier's contracts for computer security/operations services or products?	Is it standard business practice for security relevant contractual requirements including the FAR to be included in supplier's contracts for computer security/operations services or products?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
4.5.9	Budget and Resources	Procurement Controls	Do all contracts provide a means to monitor and evaluate contractor requirements, qualifications, and performance?	FAR; GISRA	Is there a policy that requires all contracts to provide a means to monitor and evaluate contractor requirements, qualifications, and performance?	Are there procedures for providing a means to monitor and evaluate contractor requirements, qualifications, and performance in all contracts?	Do all contracts provide a means to monitor and evaluate contractor requirements, qualifications, and performance?	Are periodic third party examinations conducted to verify that all contracts provide a means to monitor and evaluate contractor requirements, qualifications, and performance?	Is it standard business practice for all contracts to provide a means to monitor and evaluate contractor requirements, qualifications, and performance?
5.1.1	Life Cycle Management	System development life cycle (SDLC) methodology	Has a system development life cycle process been developed and implemented enterprise-wide?	NIST SP 800-18; OMB Cir A-130 App III; FISCAM SP-5.1	Is there a policy that requires development and implementation of a system development life cycle process enterprise-wide?	Are there procedures for developing and implementing a system development life cycle enterprise-wide?	Has a system development life cycle process been developed and implemented enterprise-wide?	Is there an independent third party review of the system development life cycle process that has been implemented enterprise-wide?	Is the use of a comprehensive system development life cycle enterprise-wide standard business practice?
5.1.2	Life Cycle Management	System development life cycle (SDLC) methodology	During system requirements analysis, are sufficient security requirements identified to mitigate known or suspected risks?	NIST SP 800-18; OMB Cir A-130 App III	Is there a policy that requires identification (during system requirements analysis) of sufficient security requirements to mitigate known or suspected risks?	Are there procedures for identifying (during system requirements analysis) sufficient security requirements to mitigate known or suspected risks?	During system requirements analysis, are sufficient security requirements identified to mitigate known or suspected risks?	Is there an independent third party review to verify that sufficient security requirements are identified to mitigate known or suspected risks?	Is it standard business practice to identify (during system requirements analysis) sufficient security requirements to mitigate known or suspected risks?
5.1.3	Life Cycle Management	System development life cycle (SDLC) methodology	Was a current risk assessment used to identify appropriate security requirements?	NIST SP 800-30; OMB Cir A-130 App III	Is there a policy that requires that a current risk assessment be used to identify appropriate security requirements?	Are there procedures for using a current risk assessment to identify appropriate security requirements?	Was a current risk assessment used to identify appropriate security requirements?	Is there an independent third party review to verify that a current risk assessment was used to identify appropriate security requirements?	Is it standard business practice to use a current risk assessment to identify appropriate security requirements?
5.1.4	Life Cycle Management	System development life cycle (SDLC) methodology	Is there a written agreement with all program officials on the risk countermeasures employed, and the extent and magnitude of the unmitigated residual risk?	NIST SP 800-18; OMB Cir A-130 App III	Is there a policy that requires a written agreement with all program officials on the risk countermeasures employed, and the extent and magnitude of the unmitigated residual risk?	Are there procedures for developing and implementing a written agreement with all program officials on the risk countermeasures employed, and the extent and magnitude of the unmitigated residual risk?	Is there a written agreement with all program officials on the risk countermeasures employed, and the extent and magnitude of the unmitigated residual risk?	Is there an independent third party review to verify that there is a written agreement with all program officials on the risk countermeasures employed, and the extent and magnitude of the unmitigated residual risk?	Is it standard business practice to have a written agreement with all program officials on the risk countermeasures employed, and the extent and magnitude of the unmitigated residual risk?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
5.1.5	Life Cycle Management	System development life cycle (SDLC) methodology	Are appropriate security controls and associated evaluation and test procedures developed prior to any procurement action?	NIST SP 800-18; OMB Cir A-130 App III	Is there a policy that requires appropriate security controls and associated evaluation and test procedures be developed prior to any procurement action?	Are there procedures for development of appropriate security controls and associated evaluation and test procedures prior to any procurement action?	Are appropriate security controls and associated evaluation and test procedures developed prior to any procurement action?	Is there a third party examination to verify that appropriate security controls and associated evaluation and test procedures have developed prior to any procurement action?	Is it standard business practice to develop appropriate security controls and associated evaluation and test procedures prior to any procurement action?
5.1.6	Life Cycle Management	System development life cycle (SDLC) methodology	Do solicitation documents (e.g., Request for Proposals) include security requirements and evaluation/test procedures?	GISRA; NIST SP 800-18	Is there a policy that requires solicitation documents (e.g., Request for Proposals) to include security requirements and evaluation/test procedures?	Are there procedures for including security requirements and evaluation/test procedures in solicitation documents (e.g., Request for Proposals)?	Do solicitation documents (e.g., Request for Proposals) include security requirements and evaluation/test procedures?	Is there an independent third party examination to verify that solicitation documents (e.g., Request for Proposals) include security requirements and evaluation/test procedures?	Is it standard business practice to include security requirements and evaluation/test procedures in solicitation documents (e.g., Request for Proposals)?
5.1.7	Life Cycle Management	System development life cycle (SDLC) methodology	Do the requirements in the solicitation documents permit and are security controls updated as new threats/vulnerabilities are identified and as new technologies are used?	NIST SP 800-18; OMB Cir A-130 App III	Is there a policy that requires requirements in the solicitation documents to permit and update security controls as new threats/vulnerabilities are identified and as new technologies are used?	Are there procedures for incorporating requirements in the solicitation documents to permit and update security controls as new threats/vulnerabilities are identified and as new technologies are used?	Do the requirements in the solicitation documents permit and are security controls updated as new threats/vulnerabilities are identified and as new technologies are used?	Is there an independent third party examination to verify that the requirements in the solicitation documents permit and update security controls as new threats/vulnerabilities are identified and as new technologies are used?	Is it standard business practice to incorporate requirements in the solicitation documents to permit and update security controls as new threats/vulnerabilities are identified and as new technologies are used?
5.1.8	Life Cycle Management	System development life cycle (SDLC) methodology	Are design reviews and system tests successfully completed prior to placing the system into production?	FISCAM CC-2.1; NIST SP 800-18; OMB Cir A-130 App III	Is there a policy that requires design reviews and system tests be successfully completed prior to placing the system into production?	Are there procedures for successfully completing design reviews and system tests prior to placing the system into production?	Are design reviews and system tests successfully completed prior to placing the system into production?	Is there an independent third party examination to verify that design reviews and system tests are successfully completed prior to placing the system into production?	Is it standard business practice to successfully complete design reviews and system tests prior to placing the system into production?
5.1.9	Life Cycle Management	System development life cycle (SDLC) methodology	If there were design constraints or design selection preferences during system design, were additional security requirements identified?	NIST SP 800-18; OMB Cir A-130 App III	Is there a policy that requires identification of additional security requirements if there were design constraints or design selection preferences during system design?	Are there procedures for identifying additional security requirements if there were design constraints or design selection preferences during system design?	If there were design constraints or design selection preferences during system design, were additional security requirements identified?	Is there an independent third party examination to verify that additional security requirements were identified If there were design constraints or design selection preferences during system design?	Is it standard business practice to identify additional security requirements if there were design constraints or design selection preferences during system design?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
5.2.1	Life Cycle Management	Changes controlled and tested through SDLC	Are system changes controlled by a formal change control process as programs progress through testing to final approval?	GISRA; NIST SP 800-18; FISCAM CC-1.1	Is there a policy that requires control of system changes by a formal change control process as programs progress through testing to final approval?	Are there procedures for controlling system changes using a formal change control process as programs progress through testing to final approval?	Are system changes controlled by a formal change control process as programs progress through testing to final approval?	Is there an independent third party examination to verify that system changes are controlled by a formal change control process as programs progress through testing to final approval?	Is it standard business practice to control system changes using a formal change control process as programs progress through testing to final approval?
5.2.2	Life Cycle Management	Changes controlled and tested through SDLC	Is all system (hardware and software) testing formalized and results recorded?	FISCAM CC-2.1; NIST SP 800-18	Is there a policy that requires all system (hardware and software) testing be formalized and results recorded?	Are there procedures for formalizing testing of all system (hardware and software) and record results?	Is all system (hardware and software) testing formalized and results recorded?	Is there an independent third party examination to verify that all system (hardware and software) testing is formalized and results recorded?	Is it standard business practice to formalize testing of all system (hardware and software) and record results?
5.2.3	Life Cycle Management	Changes controlled and tested through SDLC	Are security requirements regression tested after any modification to the system and prior to deployment?	OMB Cir A-130 App III; FISCAM CC-2.1; NIST SP 800-18	Is there a policy that requires security requirements to be regression tested after any modification to the system and prior to deployment?	Are there procedures for regression testing security requirements after any modification to the system and prior to deployment?	Are security requirements regression tested after any modification to the system and prior to deployment?	Is there an independent third party examination to verify that security requirements are regression tested after any modification to the system and prior to deployment?	Is it standard business practice to regression test security requirements after any modification to the system and prior to deployment?
5.2.4	Life Cycle Management	Changes controlled and tested through SDLC	Are changes to security options and operating system configuration parameters detected and corrected?	OMB Cir A-130 App III; FISCAM SP-2.1; NIST SP 800-18	Is there a policy that requires changes to security options and operating system configuration parameters be detected and corrected?	Are there procedures for detecting and correcting changes to security options and operating system configuration parameters?	Are changes to security options and operating system configuration parameters detected and corrected?	Is there an independent third party examination to verify that changes to security options and operating system configuration parameters are detected and corrected?	Is it standard business practice to detect and correct changes to security options and operating system configuration parameters?
5.2.5	Life Cycle Management	Changes controlled and tested through SDLC	Are new and revised hardware and software authorized, tested and approved before implementation?	NIST SP 800-18	Is there a policy that requires new and revised hardware and software be authorized, tested and approved before implementation?	Are there procedures for authorizing, testing, and approving new and revised hardware and software before implementation?	Are new and revised hardware and software authorized, tested and approved before implementation?	Is there an independent third party examination to verify that new and revised hardware and software is authorized, tested and approved before implementation?	Is it standard business practice to authorize, test, and approve new and revised hardware and software before implementation?
5.2.6	Life Cycle Management	Changes controlled and tested through SDLC	Is an impact analysis conducted to determine the effect of proposed changes on existing security controls, including the required training needed to implement the control?	NIST SP 800-18	Is there a policy that requires an impact analysis be conducted to determine the effect of proposed changes on existing security controls, including the required training needed to implement the control?	Are there procedures for conducting an impact analysis to determine the effect of proposed changes on existing security controls, including the required training needed to implement the control?	Is an impact analysis conducted to determine the effect of proposed changes on existing security controls, including the required training needed to implement the control?	Is there an independent third party examination to verify that an impact analysis was conducted to determine the effect of proposed changes on existing security controls, including the required training needed to implement the control?	Is it standard business practice to conduct an impact analysis to determine the effect of proposed changes on existing security controls, including the required training needed to implement the control?
5.2.7	Life Cycle Management	Changes controlled and tested through SDLC	Are system components formally tested and approved (operating system, utility, applications) prior to promotion to production?	NIST SP 800-18; FISCAM CC-2.1; FISCAM SS-3.1	Is there a policy that requires system components be formally tested and approved (operating system, utility, applications) prior to promotion to production?	Are there procedures for formally testing and approving system components (operating system, utility, applications) prior to promotion to production?	Are system components formally tested and approved (operating system, utility, applications) prior to promotion to production?	Is there an independent third party examination to verify that system components are formally tested and approved (operating system, utility, applications) prior to promotion to production?	Is it standard business practice to formally test and approve system components (operating system, utility, applications) prior to promotion to production?
5.2.8	Life Cycle Management	Changes controlled and tested through SDLC	Are software change request forms used to document change requests and related approvals?	NIST SP 800-18	Is there a policy that requires software change request forms be used to document change requests and related approvals?	Are there procedures for using software change request forms to document change requests and related approvals?	Are software change request forms used to document change requests and related approvals?	Is there an independent third party examination to verify that software change request forms are used to document change requests and related approvals?	Is it standard business practice to software change request forms are used to document change requests and related approvals?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
5.2.9	Life Cycle Management	Changes controlled and tested through SDLC	Are detailed system specifications prepared and reviewed by management?	FISCAM CC-2.1	Is there a policy that requires management to prepare and review detailed system specifications?	Are there procedures for management to prepare and review detailed system specifications?	Are detailed system specifications prepared and reviewed by management?	Is there an independent third party examination to verify that detailed system specifications are prepared and reviewed by management?	Is it standard business practice for management to prepare and review detailed system specifications?
5.2.10	Life Cycle Management	Changes controlled and tested through SDLC	Is the type of test data to be used specified, i.e., live or designed?	NIST SP 800-18	Is there a policy that requires specification of the type of test data to be used, i.e., live or designed?	Are there procedures for specifying the type of test data to be used, i.e., live or designed?	Is the type of test data to be used specified, i.e., live or designed?	Is there an independent third party examination to verify that the type of test data to be used is specified, i.e., live or designed?	Is it standard business practice for the type of test data to be used, i.e., live or designed to be specified?
5.2.11	Life Cycle Management	Changes controlled and tested through SDLC	Are software distribution implementation orders provided to all locations, and do these orders include an effective date?	FISCAM CC-2.3	Is there a policy that requires providing software distribution implementation orders to all locations, including an effective date?	Are there procedures for providing software distribution implementation orders to all locations, including an effective date?	Are software distribution implementation orders provided to all locations, and do these orders include an effective date?	Is there an independent third party examination to verify that software distribution implementation orders are provided to all locations, including an effective date?	Is it standard business practice to provide software distribution implementation orders to all locations, including an effective date?
5.2.12	Life Cycle Management	Changes controlled and tested through SDLC	Is there version control of all hardware and software configuration items?	NIST SP 800-18	Is there a policy that requires version control of all hardware and software configuration items?	Are there procedures for controlling the versions of all hardware and software configuration items?	Is there version control of all hardware and software configuration items?	Is there an independent third party examination to verify that there is version control of all hardware and software configuration items?	Is it standard business practice to control the versions of all hardware and software configuration items?
5.2.13	Life Cycle Management	Changes controlled and tested through SDLC	Is there a formal change control process in place for the approval of AIS or business application software changes?	NIST SP 800-18	Is there a policy that requires a formal change control process for the approval of AIS or business application software changes?	Are there procedures for using a formal change control process for the approval of AIS or business application software changes?	Is there a formal change control process in place for the approval of AIS or business application software changes?	Is there an independent third party examination to verify that a formal change control process in used for the approval of AIS or business application software changes?	Is it standard business practice to use a formal change control process for the approval of AIS or business application software changes?
5.2.14	Life Cycle Management	Changes controlled and tested through SDLC	Are all hardware and software items labeled and inventoried?	FISCAM CC-3.1	Is there a policy that requires all hardware and software items be labeled and inventoried?	Are there procedures for labeling and inventorying all hardware and software items?	Are all hardware and software items labeled and inventoried?	Is there an independent third party examination to verify that all hardware and software items are labeled and inventoried?	Is it standard business practice to label and inventory all hardware and software items?
5.2.15	Life Cycle Management	Changes controlled and tested through SDLC	Are the distribution and implementation of new or revised software documented, reviewed, and authorized?	FISCAM SS-3.2	Is there a policy that requires the distribution and implementation of new or revised software be documented, reviewed, and authorized?	Are there procedures for documenting, reviewing, and authorizing the distribution and implementation of new or revised software?	Are the distribution and implementation of new or revised software documented, reviewed, and authorized?	Is there an independent third party examination to verify that the distribution and implementation of new or revised software is documented, reviewed, and authorized?	Is it standard business practice to document, review, and authorize the distribution and implementation of new or revised software?
5.2.16	Life Cycle Management	Changes controlled and tested through SDLC	Are emergency changes documented and approved by management, either prior to the change or after the fact?	FISCAM CC-2.2	Is there a policy that requires emergency changes be documented and approved by management, either prior to the change or after the fact?	Are there procedures for management to document and approve emergency changes, either prior to the change or after the fact?	Are emergency changes documented and approved by management, either prior to the change or after the fact?	Is there an independent third party examination to verify that emergency changes are documented and approved by management, either prior to the change or after the fact?	Is it standard business practice for management to document and approve emergency changes, either prior to the change or after the fact?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
5.2.17	Life Cycle Management	Changes controlled and tested through SDLC	Are contingency plans and other associated documentation updated to reflect system changes?	NIST SP 800-18; FISCAM CC-2.1	Is there a policy that requires contingency plans and other associated documentation be updated to reflect system changes?	Are there procedures for updating contingency plans and other associated documentation to reflect system changes?	Are contingency plans and other associated documentation updated to reflect system changes?	Is there an independent third party examination to verify that contingency plans and other associated documentation are updated to reflect system changes?	Is it standard business practice for updating contingency plans and other associated documentation to reflect system changes?
5.2.18	Life Cycle Management	Changes controlled and tested through SDLC	Are software change request forms used to document requests and related approvals?	NIST SP 800-18; FISCAM CC-2.1	Is there a policy that requires using software change request forms to document requests and related approvals?	Are there procedures for using software change request forms to document requests and related approvals?	Are software change request forms used to document requests and related approvals?	Is there an independent third party examination to verify that software change request forms are used to document requests and related approvals?	Is it standard business practice to use software change request forms to document requests and related approvals?
5.2.19	Life Cycle Management	Changes controlled and tested through SDLC	Is there a configuration control board that controls all configuration changes?	NIST SP 800-18; FISCAM CC-2.1	Is there a policy that requires a controlling all configuration changes using a configuration control board?	Are there procedures for controlling all configuration changes using a configuration control board?	Is there a configuration control board that controls all configuration changes?	Is there an independent third party examination to verify that a configuration control board is controlling all configuration changes?	Is it standard business practice to control all configuration changes using a configuration control board?
5.3.1	Life Cycle Management	Security Requirements Definition	Has the data sensitivity level been identified and used in the determination of the security control mechanism?	FISCAM CC-1.1	Is there a policy that requires identification of the data sensitivity level and its use in the determination of the security control mechanism?	Are there procedures for identifying the data sensitivity level and using it in the determination of the security control mechanism?	Has the data sensitivity level been identified and used in the determination of the security control mechanism?	Is there an independent third party examination to verify that the data sensitivity level has been identified and used in the determination of the security control mechanism?	Is it standard business practice to identify the data sensitivity level and use it in the determination of the security control mechanism?
5.3.2	Life Cycle Management	Security Requirements Definition	Has a systematic review of system vulnerabilities (I.e. dial-in-access, input errors) been used to design the system security controls?	FISCAM SP-1	Is there a policy that requires using a systematic review of system vulnerabilities (I.e. dial-in-access, input errors) to design the system security controls?	Are there procedures for using a systematic review of system vulnerabilities (I.e. dial-in-access, input errors) to design the system security controls?	Has a systematic review of system vulnerabilities (I.e. dial-in-access, input errors) been used to design the system security controls?	Is there an independent third party examination to verify that a systematic review of system vulnerabilities (I.e. dial-in-access, input errors) has been used to design the system security controls?	Is it standard business practice to use a systematic review of system vulnerabilities (I.e. dial-in-access, input errors) to design the system security controls?
5.3.3	Life Cycle Management	Security Requirements Definition	Is there a system requirements document that specifies testable requirements that are not specific to a technical solution?	FISCAM SP-1	Is there a policy that requires a system requirements document that specifies testable requirements that are not specific to a technical solution?	Are there procedures for developing a system requirements document that specifies testable requirements that are not specific to a technical solution?	Is there a system requirements document that specifies testable requirements that are not specific to a technical solution?	Is there an independent third party examination to verify that the system requirements document specifies testable requirements that are not specific to a technical solution?	Is it standard business practice to develop a system requirements document that specifies testable requirements that are not specific to a technical solution?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
5.3.4	Life Cycle Management	Security Requirements Definition	Is a formal requirements review conducted with the users of the system and a security official prior to accepting the security requirements?	FISCAM SP-1	Is there a policy that requires conducting a formal requirements review with the users of the system and a security official prior to accepting the security requirements?	Are there procedures for conducting a formal requirements review with the users of the system and a security official prior to accepting the security requirements?	Is a formal requirements review conducted with the users of the system and a security official prior to accepting the security requirements?	Is there an independent third party examination to verify that a formal requirements review was conducted with the users of the system and a security official prior to accepting the security requirements?	Is it standard business practice to conduct a formal requirements review with the users of the system and a security official prior to accepting the security requirements?
5.3.5	Life Cycle Management	Security Requirements Definition	Are action items resulting from the requirements review tracked until completed?	FISCAM SP-1	Is there a policy that requires tracking action items resulting from the requirements review until completed?	Are there procedures for tracking action items resulting from the requirements review until completed?	Are action items resulting from the requirements review tracked until completed?	Is there an independent third party examination to verify that action items resulting from the requirements review are tracked until completed?	Is it standard business practice to track action items resulting from the requirements review until completed?
5.3.6	Life Cycle Management	Security Requirements Definition	Are the requirements based upon need or are they simply an automation of the way things are done?	FISCAM SP-1	Is there a policy that requires requirements to be based upon need and NOT the way things are done?	Are there procedures for identifying requirements based upon need and NOT the way things are done?	Are the requirements based upon need or are they simply an automation of the way things are done?	Is there an independent third party examination to verify that the requirements based are upon need and NOT the way things are done?	Is it standard business practice to identify requirements based upon need and NOT the way things are done?
5.4.1	Life Cycle Management	Security Design	Is a formal design review conducted with a security official prior to accepting the security design?	Best Engineering Practice	Is there a policy that requires conducting a formal design review with a security official prior to accepting the security design?	Are there procedures for conducting a formal design review with a security official prior to accepting the security design?	Is a formal design review conducted with a security official prior to accepting the security design?	Is there an independent third party examination to verify that a formal design review was conducted with a security official prior to accepting the security design?	Is it standard business practice to conduct a formal design review with a security official prior to accepting the security design?
5.4.2	Life Cycle Management	Security Design	Are action items resulting from the design review tracked until completed?	Best Engineering Practice	Is there a policy that requires tracking action items resulting from the design review until completed?	Are there procedures for tracking action items resulting from the design review until completed?	Are action items resulting from the design review tracked until completed?	Is there an independent third party examination to verify that action items resulting from the design review are tracked until completed?	Is it standard business practice to track action items resulting from the design review until completed?
5.4.3	Life Cycle Management	Security Design	Are design errors and defects tracked and measured?	Best Engineering Practice	Is there a policy that requires tracking and measuring design errors and defects?	Are there procedures for tracking and measuring design errors and defects?	Are design errors and defects tracked and measured?	Is there an independent third party examination to verify that design errors and defects tracked and measured?	Is it standard business practice to track and measure design errors and defects?
5.4.4	Life Cycle Management	Security Design	Are all design changes formally controlled through a configuration control process?	Best Engineering Practice	Is there a policy that requires formally controlling all design changes through a configuration control process?	Are there procedures for formally controlling all design changes through a configuration control process?	Are all design changes formally controlled through a configuration control process?	Is there an independent third party examination to verify that all design changes are formally controlled through a configuration control process?	Is it standard business practice to formally control all design changes through a configuration control process?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
5.4.5	Life Cycle Management	Security Design	Are consistent design review standards applied?	Best Engineering Practice	Is there a policy that requires application of consistent design review standards?	Are there procedures for developing and applying consistent design review standards?	Are consistent design review standards applied?	Is there an independent third party examination to verify that consistent design review standards are applied?	Is it standard business practice to develop and applying consistent design review standards?
5.4.6	Life Cycle Management	Security Design	Does the system design provide for the following: elimination of unnecessary programming, application of restricted user interfaces, appropriate human engineering, minimization of shared computer facilities, isolation of critical code, and appropriate backup and recovery capabilities?	Best Engineering Practice	Is there a policy that requires the system design to provide for the following: elimination of unnecessary programming, application of restricted user interfaces, appropriate human engineering, minimization of shared computer facilities, isolation of critical code, and appropriate backup and recovery capabilities?	Are there procedures for designing the system to provide for the following: elimination of unnecessary programming, application of restricted user interfaces, appropriate human engineering, minimization of shared computer facilities, isolation of critical code, and appropriate backup and recovery capabilities?	Does the system design provide for the following: elimination of unnecessary programming, application of restricted user interfaces, appropriate human engineering, minimization of shared computer facilities, isolation of critical code, and appropriate backup and recovery capabilities?	Is there an independent third party examination to verify that the system design provides for the following: elimination of unnecessary programming, application of restricted user interfaces, appropriate human engineering, minimization of shared computer facilities, isolation of critical code, and appropriate backup and recovery capabilities?	Is it standard business practice to design the system to provide for the following: elimination of unnecessary programming, application of restricted user interfaces, appropriate human engineering, minimization of shared computer facilities, isolation of critical code, and appropriate backup and recovery capabilities?
5.4.7	Life Cycle Management	Security Design	Are security requirements traced to parts of the system - operational system, physical security, software modules, or commercial products?	FISCAM AC-2	Is there a policy that requires tracing security requirements to parts of the system - operational system, physical security, software modules, or commercial products?	Are there procedures for tracing security requirements to parts of the system - operational system, physical security, software modules, or commercial products?	Are security requirements traced to parts of the system - operational system, physical security, software modules, or commercial products?	Is there an independent third party examination to verify that security requirements are traced to parts of the system - operational system, physical security, software modules, or commercial products?	Is it standard business practice to trace security requirements to parts of the system - operational system, physical security, software modules, or commercial products?
5.4.8	Life Cycle Management	Security Design	Does the security design include the following: application system interface, responsibilities associated with each interface, separation of duties, sensitive objects and operations, error tolerance, availability requirements, and requirement for basic controls.	FISCAM AC-2	Is there a policy that requires the security design to include the following: application system interface, responsibilities associated with each interface, separation of duties, sensitive objects and operations, error tolerance, availability requirements, and requirement for basic controls.	Are there procedures for including the following in the security design: application system interface, responsibilities associated with each interface, separation of duties, sensitive objects and operations, error tolerance, availability requirements, and requirement for basic controls.	Does the security design include the following: application system interface, responsibilities associated with each interface, separation of duties, sensitive objects and operations, error tolerance, availability requirements, and requirement for basic controls.	Is there an independent third party examination to verify that the security design includes the following: application system interface, responsibilities associated with each interface, separation of duties, sensitive objects and operations, error tolerance, availability requirements, and requirement for basic controls.	Is it standard business practice to include the following in the security design: application system interface, responsibilities associated with each interface, separation of duties, sensitive objects and operations, error tolerance, availability requirements, and requirement for basic controls.
5.4.9	Life Cycle Management	Security Design	Are software modules designed to accept access control adjustments based on security need?	FISCAM AC-2	Is there a policy that requires the designing software modules to accept access control adjustments based on security need?	Are there procedures for designing software modules to accept access control adjustments based on security need?	Are software modules designed to accept access control adjustments based on security need?	Is there an independent third party examination to verify that software modules are designed to accept access control adjustments based on security need?	Is it standard business practice to design software modules to accept access control adjustments based on security need?
5.4.10	Life Cycle Management	Security Design	Is there a formal design document that specifies the design and all associated interfaces?	FISCAM AC-2	Is there a policy that requires development of a formal design document that specifies the design and all associated interfaces?	Are there procedures for developing and maintaining a formal design document that specifies the design and all associated interfaces?	Is there a formal design document that specifies the design and all associated interfaces?	Is there an independent third party examination to verify that the formal design document specifies the design and all associated interfaces?	Is it standard business practice to develop and maintain a formal design document that specifies the design and all associated interfaces?
5.5.1	Life Cycle Management	Security Implementation	Is a formal implementation (code) review conducted with a security official prior to accepting the security implementation?	Best Engineering Practice	Is there a policy that requires conducting a formal implementation (code) review with a security official prior to accepting the security implementation?	Are there procedures for conducting a formal implementation (code) review with a security official prior to accepting the security implementation?	Is a formal implementation (code) review conducted with a security official prior to accepting the security implementation?	Is there an independent third party examination to verify that a formal implementation (code) review was conducted with a security official prior to accepting the security implementation?	Is it standard business practice to conduct a formal implementation (code) review with a security official prior to accepting the security implementation?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
5.5.2	Life Cycle Management	Security Implementation	Are action items resulting from the implementation (code) review tracked until completed?	Best Engineering Practice	Is there a policy that requires tracking action items resulting from the implementation (code) review until completed?	Are there procedures for tracking action items resulting from the implementation (code) review until completed?	Are action items resulting from the implementation (code) review tracked until completed?	Is there an independent third party examination to verify that action items resulting from the implementation (code) review are tracked until completed?	Is it standard business practice to track action items resulting from the implementation (code) review until completed?
5.5.3	Life Cycle Management	Security Implementation	Are implementation errors and defects tracked and measured?	Best Engineering Practice	Is there a policy that requires tracking and measuring implementation errors and defects?	Are there procedures for tracking and measuring implementation errors and defects?	Are implementation errors and defects tracked and measured?	Is there an independent third party examination to verify that implementation errors and defects are tracked and measured?	Is it standard business practice to track and measure implementation errors and defects?
5.5.4	Life Cycle Management	Security Implementation	Are all implementation changes formally controlled through a configuration control process?	Best Engineering Practice	Is there a policy that requires formally controlling all implementation changes through a configuration control process?	Are there procedures for formally controlling all implementation changes through a configuration control process?	Are all implementation changes formally controlled through a configuration control process?	Is there an independent third party examination to verify that all implementation changes are formally controlled through a configuration control process?	Is it standard business practice to formally control all implementation changes through a configuration control process?
5.5.5	Life Cycle Management	Security Implementation	Are consistent implementation standards applied?	Best Engineering Practice	Is there a policy that requires application of consistent implementation standards?	Are there procedures for applying consistent implementation standards?	Are consistent implementation standards applied?	Is there an independent third party examination to verify that consistent implementation standards are applied?	Is it standard business practice to apply consistent implementation standards?
5.5.6	Life Cycle Management	Security Implementation	Are the size and complexity of each implementation component evaluated and tracked over time?	Best Engineering Practice	Is there a policy that requires evaluating and tracking the size and complexity of each implementation component over time?	Are there procedures for evaluating and tracking the size and complexity of each implementation component over time?	Are the size and complexity of each implementation component evaluated and tracked over time?	Is there an independent third party examination to verify that the size and complexity of each implementation component is evaluated and tracked over time?	Is it standard business practice to evaluate and track the size and complexity of each implementation component over time?
5.5.7	Life Cycle Management	Security Implementation	Are potential vulnerabilities documented and addressed throughout the implementation phase?	FISCAM AC-2	Is there a policy that requires documenting and addressing potential vulnerabilities throughout the implementation phase?	Are there procedures for documenting and addressing potential vulnerabilities throughout the implementation phase?	Are potential vulnerabilities documented and addressed throughout the implementation phase?	Is there an independent third party examination to verify that potential vulnerabilities are documented and addressed throughout the implementation phase?	Is it standard business practice to document and address potential vulnerabilities throughout the implementation phase?
5.5.8	Life Cycle Management	Security Implementation	Is data transfer using files accomplished in a secure fashion?	Best Engineering Practice	Is there a policy that requires accomplishing data transfer using files in a secure fashion?	Are there procedures for accomplishing data transfer using files in a secure fashion?	Is data transfer using files accomplished in a secure fashion?	Is there an independent third party examination to verify that data transfer using files is accomplished in a secure fashion?	Is it standard business practice to accomplish data transfer using files in a secure fashion?
5.5.9	Life Cycle Management	Security Implementation	Are there mechanisms in place to ensure that information stored in memory cannot be accessed except by software/users that are permitted access?	Best Engineering Practice	Is there a policy that requires mechanisms to ensure that information stored in memory cannot be accessed except by software/users that are permitted access?	Are there procedures for using mechanisms to ensure that information stored in memory cannot be accessed except by software/users that are permitted access?	Are there mechanisms in place to ensure that information stored in memory cannot be accessed except by software/users that are permitted access?	Is there an independent third party examination to verify that there are mechanisms in place to ensure that information stored in memory cannot be accessed except by software/users that are permitted access?	Is it standard business practice to use mechanisms to ensure that information stored in memory cannot be accessed except by software/users that are permitted access?
5.5.10	Life Cycle Management	Security Implementation	Is all code documented?	Best Engineering Practice	Is there a policy that requires documentation of all code?	Are there procedures for documenting all code?	Is all code documented?	Is there an independent third party examination to verify that all code is documented?	Is it standard business practice to document all code?
5.6.1	Life Cycle Management	Security Testing	Is a formal testing review conducted with a security official prior to accepting the security testing results?	Best Engineering Practice	Is there a policy that requires conducting a formal testing review with a security official prior to accepting the security testing results?	Are there procedures for conducting a formal testing review with a security official prior to accepting the security testing results?	Is a formal testing review conducted with a security official prior to accepting the security testing results?	Is there an independent third party examination to verify that a formal testing review was conducted with a security official prior to accepting the security testing results?	Is it standard business practice to conduct a formal testing review with a security official prior to accepting the security testing results?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
5.6.2	Life Cycle Management	Security Testing	Are action items resulting from the testing review tracked until completed?	Best Engineering Practice	Is there a policy that requires tracking action items from the testing review until completed?	Are there procedures for tracking action items from the testing review until completed?	Are action items resulting from the testing review tracked until completed?	Is there an independent third party examination to verify that action items resulting from the testing review are tracked until completed?	Is it standard business practice to track action items from the testing review until completed?
5.6.3	Life Cycle Management	Security Testing	Are testing errors and defects tracked and measured?	Best Engineering Practice	Is there a policy that requires tracking and measuring testing errors and defects?	Are there procedures for tracking and measuring testing errors and defects?	Are testing errors and defects tracked and measured?	Is there an independent third party examination to verify that testing errors and defects are tracked and measured?	Is it standard business practice to track and measure testing errors and defects?
5.6.4	Life Cycle Management	Security Testing	Are all testing changes formally controlled through a configuration control process?	Best Engineering Practice	Is there a policy that requires formally controlled all testing changes through a configuration control process?	Are there procedures for formally controlled all testing changes through a configuration control process?	Are all testing changes formally controlled through a configuration control process?	Is there an independent third party examination to verify that all testing changes are formally controlled through a configuration control process?	Is it standard business practice to formally control all testing changes through a configuration control process?
5.6.5	Life Cycle Management	Security Testing	Are consistent testing standards applied?	Best Engineering Practice	Is there a policy that requires application of consistent testing standards?	Are there procedures for applying consistent testing standards?	Are consistent testing standards applied?	Is there an independent third party examination to verify that consistent testing standards are applied?	Is it standard business practice to apply consistent testing standards?
5.6.6	Life Cycle Management	Security Testing	Is the size and complexity of each testing component evaluated and tracked over time?	Best Engineering Practice	Is there a policy that requires evaluating and tracking the size and complexity of each testing component over time?	Are there procedures for evaluating and tracking the size and complexity of each testing component over time?	Is the size and complexity of each testing component evaluated and tracked over time?	Is there an independent third party examination to verify that the size and complexity of each testing component evaluated and tracked over time?	Is it standard business practice to evaluate and track the size and complexity of each testing component over time?
5.6.7	Life Cycle Management	Security Testing	Is boundary testing performed?	Best Engineering Practice	Is there a policy that requires performance of boundary testing?	Are there procedures for performing boundary testing?	Is boundary testing performed?	Is there an independent third party examination to verify that boundary testing is performed?	Is it standard business practice to perform boundary testing?
5.6.8	Life Cycle Management	Security Testing	Is there a detailed test plan that identifies the requirements to be tested and how they are to be tested?	Best Engineering Practice	Is there a policy that requires development and maintenance of a detailed test plan that identifies the requirements to be tested and how they are to be tested?	Are there procedures for developing and maintaining a detailed test plan that identifies the requirements to be tested and how they are to be tested?	Is there a detailed test plan that identifies the requirements to be tested and how they are to be tested?	Is there an independent third party examination to verify that there is a detailed test plan that identifies the requirements to be tested and how they are to be tested?	Is it standard business practice to develop and maintain a detailed test plan that identifies the requirements to be tested and how they are to be tested?
5.6.9	Life Cycle Management	Security Testing	When the creation of test data is not feasible and the use of production data is needed for testing, is the production data protected and controlled?	Best Engineering Practice	Is there a policy that requires protecting and controlling any production data needed for testing?	Are there procedures for protecting and controlling any production data used for testing?	When the creation of test data is not feasible and the use of production data is needed for testing, is the production data protected and controlled?	Is there an independent third party examination to verify that production data is protected and controlled when used for testing?	Is it standard business practice to protect and control any production data used for testing?
5.6.10	Life Cycle Management	Security Testing	Is there software testing of all inbound information to ensure exclusion of any data that does not fit the requirements for acceptable data?	Best Engineering Practice	Is there a policy that requires software testing of all inbound information to ensure exclusion of any data that does not fit the requirements for acceptable data?	Are there procedures for software testing of all inbound information to ensure exclusion of any data that does not fit the requirements for acceptable data?	Is there software testing of all inbound information to ensure exclusion of any data that does not fit the requirements for acceptable data?	Is there an independent third party examination to verify that there is software testing of all inbound information to ensure exclusion of any data that does not fit the requirements for acceptable data?	Is it standard business practice to perform software testing on all inbound information to ensure exclusion of any data that does not fit the requirements for acceptable data?
5.6.11	Life Cycle Management	Security Testing	Are multiple levels of testing performed, such as module level, system level, and acceptance testing?	Best Engineering Practice	Is there a policy that requires performance of multiple levels of testing, such as module level, system level, and acceptance testing?	Are there procedures for performing multiple levels of testing, such as module level, system level, and acceptance testing?	Are multiple levels of testing performed, such as module level, system level, and acceptance testing?	Is there an independent third party examination to verify that multiple levels of testing are performed, such as module level, system level, and acceptance testing?	Is it standard business practice to perform multiple levels of testing, such as module level, system level, and acceptance testing?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
5.7.1	Life Cycle Management	Security Deployment	Is there a deployment plan that specifies deployment procedures, locations, schedules, and responsibilities?	Best Engineering Practice	Is there a policy that requires development and maintenance of a deployment plan that specifies deployment procedures, locations, schedules, and responsibilities?	Are there procedures for developing and maintaining a deployment plan that specifies deployment procedures, locations, schedules, and responsibilities?	Is there a deployment plan that specifies deployment procedures, locations, schedules, and responsibilities?	Is there an independent third party examination to verify that the deployment plan specifies deployment procedures, locations, schedules, and responsibilities?	Is it standard business practice to develop and maintain a deployment plan that specifies deployment procedures, locations, schedules, and responsibilities?
5.7.2	Life Cycle Management	Security Deployment	Are systems formally accepted by the configuration control board prior to deployment?	Best Engineering Practice	Is there a policy that requires the configuration control board to formally accept systems formally accepted by the prior to deployment?	Are there procedures for using a configuration control board to formally accept systems formally accepted by the prior to deployment?	Are systems formally accepted by the configuration control board prior to deployment?	Is there an independent third party examination to verify that systems are formally accepted by the configuration control board prior to deployment?	Is it standard business practice to use a configuration control board to formally accept systems formally accepted by the prior to deployment?
5.7.3	Life Cycle Management	Security Deployment	Is a formal deployment review conducted with a security official prior to accepting the security deployment plan?	Best Engineering Practice	Is there a policy that requires conducting a formal deployment review with a security official prior to accepting the security deployment plan?	Are there procedures for conducting a formal deployment review with a security official prior to accepting the security deployment plan?	Is a formal deployment review conducted with a security official prior to accepting the security deployment plan?	Is there an independent third party examination to verify that a formal deployment review is conducted with a security official prior to accepting the security deployment plan?	Is it standard business practice to conduct a formal deployment review with a security official prior to accepting the security deployment plan?
5.7.4	Life Cycle Management	Security Deployment	Are action items resulting from the deployment review tracked until completed?	Best Engineering Practice	Is there a policy that requires tracking action items resulting from the deployment review until completed?	Are there procedures for tracking action items resulting from the deployment review until completed?	Are action items resulting from the deployment review tracked until completed?	Is there an independent third party examination to verify that action items resulting from the deployment review are tracked until completed?	Is it standard business practice to track action items resulting from the deployment review until completed?
5.7.5	Life Cycle Management	Security Deployment	Are deployment errors and defects tracked and measured?	Best Engineering Practice	Is there a policy that requires tracking and measuring deployment errors and defects?	Are there procedures for tracking and measuring deployment errors and defects?	Are deployment errors and defects tracked and measured?	Is there an independent third party examination to verify that deployment errors and defects are tracked and measured?	Is it standard business practice to track and measure deployment errors and defects?
5.7.6	Life Cycle Management	Security Deployment	Are all deployment changes formally controlled through a configuration control process?	Best Engineering Practice	Is there a policy that requires formally controlling all deployment changes through a configuration control process?	Are there procedures for formally controlling all deployment changes through a configuration control process?	Are all deployment changes formally controlled through a configuration control process?	Is there an independent third party examination to verify that all deployment changes are formally controlled through a configuration control process?	Is it standard business practice to formally control all deployment changes through a configuration control process?
5.7.7	Life Cycle Management	Security Deployment	Are consistent deployment standards applied?	Best Engineering Practice	Is there a policy that requires application of consistent deployment standards?	Are there procedures for applying consistent deployment standards?	Are consistent deployment standards applied?	Is there an independent third party examination to verify that consistent deployment standards are applied?	Is it standard business practice to apply consistent deployment standards?
5.7.8	Life Cycle Management	Security Deployment	Are user manuals that specify procedures and responsibilities provided as part of the deployment?	Best Engineering Practice	Is there a policy that requires providing user manuals that specify procedures and responsibilities as part of the deployment?	Are there procedures for providing user manuals that specify procedures and responsibilities as part of the deployment?	Are user manuals that specify procedures and responsibilities provided as part of the deployment?	Is there an independent third party examination to verify that user manuals that specify procedures and responsibilities are provided as part of the deployment?	Is it standard business practice to provide user manuals that specify procedures and responsibilities as part of the deployment?
6.1.1	Incident and Emergency Response	Critical and sensitive assets Identification	Has the sensitivity of the information contained on each system been determined?	FISCAM AC-1.2; NIST SP 800-18; OMB Cir A-130 App III; FISCAM AC-1.1	Is there a policy that requires determination of the sensitivity of the information contained on each system?	Are there procedures for determining the sensitivity of the information contained on each system?	Has the sensitivity of the information contained on each system been determined?	Are there periodic reviews to verify the sensitivity of the information contained on each system?	Is it standard business practice to determine the sensitivity of the information contained on each system?
6.1.2	Incident and Emergency Response	Critical and sensitive assets Identification	Have the operations and their supporting computer resources most critical and sensitive to the agency or national mission been identified?	OMB Cir A-130 App III	Is there a policy that requires identification of the operations and their supporting computer resources most critical and sensitive to the agency or national mission?	Are there procedures for identifying the operations and their supporting computer resources most critical and sensitive to the agency or national mission?	Have the operations and their supporting computer resources most critical and sensitive to the agency or national mission been identified?	Are there periodic third party reviews to verify that the operations and their supporting computer resources most critical and sensitive to the agency or national mission been identified?	Is it standard business practice to identify the operations and their supporting computer resources most critical and sensitive to the agency or national mission been identified?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
6.2.1	Incident and Emergency Response	Contingency/ disaster response	Is there a current (updated within the past year) contingency plan?	FISCAM SC-3.1; OMB Cir A-130 App III; NIST SP 800-18	Is there a policy that requires a current (updated within the past year) contingency plan?	Are there procedures for developing and maintaining (updated within the past year) a contingency plan?	Is there a current (updated within the past year) contingency plan?	Has the contingency plan been tested as extensively as possible (in an operational versus simulated fashion)?	Is it standard business practice to maintain current (updated within the past year) contingency plans?
6.2.2	Incident and Emergency Response	Contingency/ disaster response	If an alternate processing and telecommunication site is not agency owned, is there a contract or inter-agency agreement in place?	NIST SP 800-18	Is there a policy that requires an in place contract or inter-agency agreement for any alternate processing and telecommunication site not agency owned?	Are there procedures for developing and maintaining an in place contract or inter-agency agreement for any alternate processing and telecommunication site not agency owned?	If an alternate processing and telecommunication site is not agency owned, is there a contract or inter-agency agreement in place?	Is there a periodic third party review to verify that if an alternate processing and telecommunication site is not agency owned, is there a contract or inter-agency agreement in place?	Is it standard business practice to have an in place contract or inter-agency agreement for any alternate processing and telecommunication site not agency owned?
6.2.3	Incident and Emergency Response	Contingency/ disaster response	Do key affected parties approve the contingency plan?	FISCAM SC-3.1	Is there a policy that requires approval of the contingency plan by key affected parties?	Are there procedures for obtaining approval of the contingency plan by key affected parties?	Do key affected parties approve the contingency plan?	Is there a periodic third party review to verify that key affected parties approve the contingency plan?	Is it standard business practice to ensure key affected parties approve the contingency plan?
6.2.4	Incident and Emergency Response	Contingency/ disaster response	Are responsibilities for emergency recovery of operations assigned?	FISCAM SC-3	Is there a policy that requires assignment of responsibilities for emergency recovery of operations?	Are there procedures for assigning responsibilities for emergency recovery of operations?	Are responsibilities for emergency recovery of operations assigned?	Is there a periodic third party review to verify that responsibilities for emergency recovery of operations are assigned?	Is it standard business practice to assign responsibilities for emergency recovery of operations?
6.2.5	Incident and Emergency Response	Contingency/ disaster response	Are there current detailed instructions for restoring operations?	FISCAM SC-3	Is there a policy that requires current detailed instructions for restoring operations?	Are there procedures for developing and maintaining detailed instructions for restoring operations?	Are there current detailed instructions for restoring operations?	Have the detailed instructions for restoring operations been tested (within the past year) as realistically as possible?	Is it standard business practice to have current detailed instructions for restoring operations?
6.2.6	Incident and Emergency Response	Contingency/ disaster response	Is there an alternate processing and telecommunication site?	NIST SP 800-18	Is there a policy that requires an alternate processing and telecommunication site?	Are there procedures for obtaining and using an alternate processing and telecommunication site?	Is there an alternate processing and telecommunication site?	Have operations from any alternate processing and telecommunication sites been thoroughly tested within the past year?	Is it standard business practice to have an alternate processing and telecommunication site?
6.2.7	Incident and Emergency Response	Contingency/ disaster response	Are backups stored at a location known to all personnel involved in generating and restoring backups?	NIST SP 800-18	Is there a policy that requires backups be stored at a location known to all personnel involved in generating and restoring backups?	Are there procedures for storing backups at a location known to all personnel involved in generating and restoring backups?	Are backups stored at a location known to all personnel involved in generating and restoring backups?	Is there a periodic third party review to verify that backups are stored at a location known to all personnel involved in generating and restoring backups?	Is it standard business practice to store backups at a location known to all personnel involved in generating and restoring backups?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
6.2.8	Incident and Emergency Response	Contingency/ disaster response	Is system and application documentation maintained at an off-site or alternate location?	FISCAM SC-2.1	Is there a policy that requires system and application documentation be maintained at an off-site or alternate location?	Are there procedures for maintaining system and application documentation at an off-site or alternate location?	Is system and application documentation maintained at an off site or alternate location?	Is there a periodic third party examination to verify system and application documentation is maintained at an off-site or alternate location?	Is it standards business practice to maintain system and application documentation at an off-site or alternate location?
6.2.9	Incident and Emergency Response	Contingency/ disaster response	Are all system (MA and GSS) settings restored to their previous state (NOT reset to product defaults) after being restored from a backup?	NIST SP 800-18	Is there a policy that requires all system (MA and GSS) settings be restored to their previous state (NOT reset to product defaults) after being restored from a backup?	Are there procedures for restoring all system (MA and GSS) settings to their previous state (NOT reset to product defaults) after being restored from a backup?	Are all system (MA and GSS) settings restored to their previous state (NOT reset to product defaults) after being restored from a backup?	Is there a periodic third party review to verify that all system (MA and GSS) settings are restored to their previous state (NOT reset to product defaults) after being restored from a backup?	Is it standards business practice to restore all system (MA and GSS) settings restored to their previous state (NOT reset to product defaults) after being restored from a backup?
6.2.10	Incident and Emergency Response	Contingency/ disaster response	Are the backup storage site and alternate operational site geographically removed from the primary site and physically protected?	FISCAM SC-2.1	Is there a policy that requires the backup storage site and alternate operational site be geographically removed from the primary site and physically protected?	Are there procedures for establishing and maintaining the backup storage site and alternate operational site in a location geographically removed from the primary site and physically protected?	Are the backup storage site and alternate operational site geographically removed from the primary site and physically protected?	Is there a periodic third party review to verify that the backup storage site and alternate operational site are geographically removed from the primary site and physically protected?	Is it standards business practice to establish and maintain the backup storage site and alternate operational site in a location geographically removed from the primary site and physically protected?
6.2.11	Incident and Emergency Response	Contingency/ disaster response	Has the current version of the contingency plan been distributed to all appropriate personnel?	FISCAM SC-3.1	Is there a policy that requires the current version of the contingency plan to be distributed to all appropriate personnel? Does the policy identify the appropriate personnel?	Are there procedures for distributing the current version of the contingency plan to all appropriate personnel?	Has the current version of the contingency plan been distributed to all appropriate personnel?	Is there a periodic third party review to verify that the current version of the contingency plan has been distributed to all appropriate personnel?	Is it standards business practice to distribute the current version of the contingency plan to all appropriate personnel?
6.2.12	Incident and Emergency Response	Contingency/ disaster response	Is a current disaster recovery plan in place?	FISCAM SC-3.1	Is there a policy that requires a current disaster recovery plan?	Are there procedures for establishing and maintaining a current disaster recovery plan?	Is a current disaster recovery plan in place?	Is there a periodic third party review to verify that a current disaster recovery plan is in place?	Is it standards business practice to have current disaster recovery plan in place?
6.2.13	Incident and Emergency Response	Contingency/ disaster response	Is the current contingency plan/disaster recovery plan stored off-site?	FISCAM SC-3.1	Is there a policy that requires storage of the current contingency plan/disaster recovery plan off-site?	Are there procedures for storing the current contingency plan/disaster recovery plan off-site?	Is the current contingency plan/disaster recovery plan stored off-site?	Is there a periodic third party review to verify that the current contingency plan/disaster recovery plan is stored off-site?	Is it standards business practice to store the current contingency plan/disaster recovery plan off-site?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
6.2.14	Incident and Emergency Response	Contingency/ disaster response	Are employees recently (within the past year) trained in their disaster response roles and responsibilities?	NIST SP 800-18; FISCAM SC-2.3	Is there a policy that requires employees to be recently (within the past year) trained in their disaster response roles and responsibilities?	Are there procedures for training employees in their disaster response roles and responsibilities?	Are employees recently (within the past year) trained in their disaster response roles and responsibilities?	Is there a periodic third party review to verify that employees have been recently (within the past year) trained in their disaster response roles and responsibilities?	Is it standards business practice to train employees in their disaster response roles and responsibilities on a yearly basis?
6.2.15	Incident and Emergency Response	Contingency/ disaster response	Is the contingency plan modified based upon results of realistic testing?	NIST SP 800-18	Is there a policy that requires the contingency plan to be modified based upon results of realistic testing?	Are there procedures for modifying the contingency plan based upon results of realistic testing?	Is the contingency plan modified based upon results of realistic testing?	Is there a periodic third party review to verify that the contingency plan has been modified based upon results of realistic testing?	Is it standards business practice to modify the contingency plan based upon results of realistic testing?
6.2.16	Incident and Emergency Response	Contingency/ disaster response	Is the disaster recovery plan modified based upon results of realistic testing?	NIST SP 800-18	Is there a policy that requires the disaster recovery plan to be modified based upon results of realistic testing?	Are there procedures for modifying the disaster recovery plan based upon results of realistic testing?	Is the disaster recovery plan modified based upon results of realistic testing?	Is there a periodic third party review to verify that the disaster recovery plan has been modified based upon results of realistic testing?	Is it standards business practice to modify the disaster recovery plan based upon results of realistic testing?
6.2.17	Incident and Emergency Response	Contingency/ disaster response	Can emergency appropriations be obtained, yet expenditures be controlled, in the event of a disaster?	FISCAM SC-3.1	Is there a policy that requires a mechanism for obtaining emergency appropriations while controlling expenditures, in the event of a disaster?	Are there procedures for obtaining emergency appropriations while controlling expenditures, in the event of a disaster?	Can emergency appropriations be obtained, yet expenditures be controlled, in the event of a disaster?	Has the mechanism for obtaining emergency appropriations while controlling expenditures, in the event of a disaster been tested?	Is it standards business practice to be able to obtain emergency appropriations while controlling expenditures, in the event of a disaster?
6.2.18	Incident and Emergency Response	Contingency/ disaster response	Does the contingency plan address responses to utility outages such as electricity, water, gas, etc?	NIST SP 800-14; FISCAM SC-3	Is there a policy that requires the contingency plan to address responses to utility outages such as electricity, water, gas, etc?	Are there procedures for addressing responses to utility outages such as electricity, water, gas, etc. in the contingency plan?	Does the contingency plan address responses to utility outages such as electricity, water, gas, etc?	Is there a periodic third party review to verify that the contingency plan addresses responses to utility outages such as electricity, water, gas, etc?	Is it standards business practice to address responses to utility outages such as electricity, water, gas, etc. in the contingency plan?
6.2.19	Incident and Emergency Response	Contingency/ disaster response	Does the contingency plan address coordination with fire/medical/security service providers?	NIST SP 800-14; NIST SP 800-18; FISCAM SC-2; FISCAM SC-3	Is there a policy that requires addressing coordination with fire/medical/security service providers in the contingency plan?	Are there procedures for addressing coordination with fire/medical/security service providers in the contingency plan?	Does the contingency plan address coordination with fire/medical/security service providers?	Is there a periodic third party review to verify that the contingency plan addresses coordination with fire/medical/security service providers?	Is it standards business practice to address coordination with fire/medical/security service providers in the contingency plan?
6.2.20	Incident and Emergency Response	Contingency/ disaster response	Are critical files backed up on a regular basis?	NIST SP 800-14; FISCAM SC-2	Is there a policy that requires backing up critical files on a regular basis? Does the policy specify the frequency of backup?	Are there procedures for backing up critical files on a regular basis?	Are critical files backed up on a regular basis?	Is there a periodic third party tests to verify that critical files are backed up on a regular basis?	Is it standards business practice to verify that critical files are backed up on a regular basis?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
6.2.21	Incident and Emergency Response	Contingency/ disaster response	Is test data maintained off-site for each critical system so that in the event of a disaster, the recovered system can be tested to ensure that it functions properly?	NIST SP 800-14; FISCAM SC-2	Is there a policy that requires maintenance of test data off-site for each critical system so that in the event of a disaster, the recovered system can be tested to ensure that it functions properly?	Are there procedures for maintaining test data off-site for each critical system so that in the event of a disaster, the recovered system can be tested to ensure that it functions properly?	Is test data maintained off-site for each critical system so that in the event of a disaster, the recovered system can be tested to ensure that it functions properly?	Is there a periodic third party review to verify that test data is maintained off-site for each critical system so that in the event of a disaster, the recovered system can be tested to ensure that it functions properly?	Is it standards business practice to maintain test data off-site for each critical system so that in the event of a disaster, the recovered system can be tested to ensure that it functions properly?
6.2.22	Incident and Emergency Response	Contingency/ disaster response	Are affected organizations notified of delays or other problems in the event of a critical system failure or a telecommunications failure?	NIST SP 800-14; FISCAM SC-2	Is there a policy that requires notification to affected organizations regarding delays or other problems in the event of a critical system failure or a telecommunications failure?	Are there procedures for notifying affected organizations regarding delays or other problems in the event of a critical system failure or a telecommunications failure?	Are affected organizations notified of delays or other problems in the event of a critical system failure or a telecommunications failure?	Has a test been conducted to verify that affected organizations are notified of delays or other problems in the event of a critical system failure or a telecommunications failure?	Is it standards business practice to notify affected organizations of delays or other problems in the event of a critical system failure or a telecommunications failure?
6.2.23	Incident and Emergency Response	Contingency/ disaster response	Have written arrangements been made with HW/SW vendors of critical system components for priority-level support in the event of a disaster?	NIST SP 800-14; FISCAM SC-2	Is there a policy that requires written arrangements with HW/SW vendors of critical system components for priority-level support in the event of a disaster?	Are there procedures for making written arrangements with HW/SW vendors of critical system components for priority-level support in the event of a disaster?	Have written arrangements been made with HW/SW vendors of critical system components for priority-level support in the event of a disaster?	Is there a periodic third party review to verify that written arrangements have been made with HW/SW vendors of critical system components for priority-level support in the event of a disaster?	Is it standard business practice to have written arrangements with HW/SW vendors of critical system components for priority-level support in the event of a disaster?
6.2.24	Incident and Emergency Response	Contingency/ disaster response	Do the contingency/disaster recovery plans include responding to problems with air/ground transportation systems?	NIST SP 800-14; FISCAM SC-2	Is there a policy that requires contingency/disaster recovery plans to include responding to problems with air/ground transportation systems?	Are there procedures for including responding to problems with air/ground transportation systems in contingency/disaster recovery plans?	Do the contingency/disaster recovery plans include responding to problems with air/ground transportation systems?	Is there a periodic third party review to verify that the contingency/disaster recovery plans include responding to problems with air/ground transportation systems?	Is it standard business practice to include responding to problems with air/ground transportation systems in the contingency/disaster recovery plans?
6.2.25	Incident and Emergency Response	Contingency/ disaster response	Are copies of critical forms and vital documents stored at a safe and accessible backup site?	NIST SP 800-12; FISCAM SC-2	Is there a policy that requires storage of copies of critical forms and vital documents at a safe and accessible backup site?	Are there procedures for storing copies of critical forms and vital documents at a safe and accessible backup site?	Are copies of critical forms and vital documents stored at a safe and accessible backup site?	Is there a periodic third party review to verify that copies of critical forms and vital documents are stored at a safe and accessible backup site?	Is it standard business practice to store copies of critical forms and vital documents at a safe and accessible backup site?
6.2.26	Incident and Emergency Response	Contingency/ disaster response	Are backups generated and labeled such that full system restores are possible for system states between the present and 3 months past?	NIST SP 800-18	Is there a policy that requires generation and labeling of backups such that full system restores are possible for system states between the present and 3 months past?	Are there procedures for generation and labeling of backups such that full system restores are possible for system states between the present and 3 months past?	Are backups generated and labeled such that full system restores are possible for system states between the present and 3 months past?	Is there a periodic third party test to verify that full system restores are possible for system states between the present and 3 months past?	Is it standard business practice to generate and label backups such that full system restores are possible for system states between the present and 3 months past?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
6.3.1	Incident and Emergency Response	Incident identification, reporting and response	Are intrusion detection reports routinely reviewed and suspected incidents handled accordingly?	NIST SP 800-18	Is there a policy that requires reviewing intrusion detection reports routinely and handling suspected incidents accordingly?	Are there procedures for reviewing intrusion detection reports routinely and handling suspected incidents accordingly?	Are intrusion detection reports routinely reviewed and suspected incidents handled accordingly?	Have periodic tests been conducted by an independent third party to verify that intrusion detection reports are routinely reviewed and suspected incidents handled accordingly?	Is it standard business practice to review intrusion detection reports routinely and handle suspected incidents accordingly?
6.3.2	Incident and Emergency Response	Incident identification, reporting and response	Are users provided assistance during recovery from a security incident?	FISCAM SP-4.1; NIST SP 800-18; OMB Cir A-130 App III	Is there a policy that requires users be provided assistance during recovery from a security incident?	Are there procedures for providing assistance to users during recovery from a security incident?	Are users provided assistance during recovery from a security incident?	Have periodic tests been conducted by an independent third party to verify that users are provided assistance during recovery from a security incident?	Is it standard business practice to provide users with assistance during recovery from a security incident?
6.3.3	Incident and Emergency Response	Incident identification, reporting and response	Is there a formal incident response capability?	NIST SP 800-18; FISCAM SP-3.4	Is there a policy that requires a formal incident response capability?	Are there procedures for providing a formal incident response capability?	Is there a formal incident response capability?	Have periodic tests been conducted by an independent third party to verify that there is a formal incident response capability?	Is it standard business practice to have a formal incident response capability?
6.3.4	Incident and Emergency Response	Incident identification, reporting and response	Are all employees responsible for incident reporting?	NIST SP 800-18; FISCAM SP-3.4	Is there a policy that requires all employees to be responsible for incident reporting?	Are there procedures for employees to report incidents?	Are all employees responsible for incident reporting?	Have periodic tests been conducted by an independent third party to verify that all employees report incidents?	Is it standard business practice to have all employees responsible for reporting incidents?
6.3.5	Incident and Emergency Response	Incident identification, reporting and response	Is emergency response corrective action monitored and tracked until resolved?	NIST SP 800-18	Is there a policy that requires monitoring and tracking emergency response corrective action until resolved?	Are there procedures for monitoring and tracking emergency response corrective action until resolved?	Is emergency response corrective action monitored and tracked until resolved?	Have periodic examinations been performed by an independent third party to verify that emergency response corrective actions are monitored and tracked until resolved?	Is it standard business practice to monitor and track emergency response corrective actions?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
6.3.6	Incident and Emergency Response	Incident identification, reporting and response	Are alerts/advisories received and responded to appropriately?	NIST SP 800-18	Is there a policy that requires receiving and appropriately responding to alerts/advisories?	Are there procedures for receiving and appropriately responding to alerts/advisories?	Are alerts/advisories received and responded to appropriately?	Have periodic tests been conducted by an independent third party to verify that alerts/advisories are received and responded to appropriately?	Is it standard business practice to receive and appropriately respond to alerts/advisories?
6.3.7	Incident and Emergency Response	Incident identification, reporting and response	Is incident handling modified to improve the incident handling capability based on lessons learned from past experience?	NIST SP 800-18	Is there a policy that requires updating the incident handling capability based on lessons learned from past experience?	Are there procedures for updating the incident handling capability based on lessons learned from past experience?	Is incident handling modified to improve the incident handling capability based on lessons learned from past experience?	Have periodic examinations been performed by an independent third party to verify that incident handling has been modified to improve the incident handling capability based on lessons learned from past experience?	Is it standard business practice to improve the incident handling capability based on lessons learned from past experience?
6.3.8	Incident and Emergency Response	Incident identification, reporting and response	Is incident related information shared with interconnected organizations?	NIST SP 800-18	Is there a policy that requires sharing incident related information with interconnected organizations?	Are there procedures for sharing incident related information with interconnected organizations?	Is incident related information shared with interconnected organizations?	Have periodic tests been conducted by an independent third party to verify that incident related information is shared with interconnected organizations?	Is it standard business practice to share incident related information with interconnected organizations?
6.3.9	Incident and Emergency Response	Incident identification, reporting and response	Is incident evidence preserved?	NIST SP 800-18	Is there a policy that requires incident evidence preservation?	Are there procedures for preservation of incident evidence?	Is incident evidence preserved?	Have periodic tests been conducted by an independent third party to verify that incident evidence is preserved?	Is it standard business practice to preserve incident evidence?
6.3.10	Incident and Emergency Response	Incident identification, reporting and response	Are incident related vulnerabilities and threat sources shared with FedCIRC?	OMB Cir A-130 App III	Is there a policy that requires sharing incident related vulnerabilities and threat sources with FedCIRC?	Are there procedures for sharing incident related vulnerabilities and threat sources with FedCIRC?	Are incident related vulnerabilities and threat sources shared with FedCIRC?	Have tests been conducted to verify that incident related vulnerabilities and threat sources are shared with FedCIRC?	Is it standard business practice to share incident related vulnerabilities and threat sources with FedCIRC?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
6.3.11	Incident and Emergency Response	Incident identification, reporting and response	Is incident occurrence reported to FedCIRC, NIPC, and, if necessary, law enforcement?	OMB Cir A-130 App III	Is there a policy that requires reporting incident occurrence to FedCIRC, NIPC, and, if necessary, law enforcement?	Are there procedures for reporting incident occurrence to FedCIRC, NIPC, and, if necessary, law enforcement?	Is incident occurrence reported to FedCIRC, NIPC, and, if necessary, law enforcement?	Have tests been conducted to verify that incident occurrence is reported to FedCIRC, NIPC, and, if necessary, law enforcement?	Is it standard business practice to report incident occurrence to FedCIRC, NIPC, and, if necessary, law enforcement?
6.3.12	Incident and Emergency Response	Incident identification, reporting and response	Are suspected incidents reported, investigated, responded to, and corrective action taken (including penalties)?	FISCAM AC-4.3	Is there a policy that requires reporting, investigating, responding to, and taking corrective action (including penalties) on all suspected incidents?	Are there procedures for reporting, investigating, responding to, and taking corrective action (including penalties) on all suspected incidents?	Are suspected incidents reported, investigated, responded to, and corrective action taken (including penalties)?	Have periodic tests been conducted by an independent third party to verify that suspected incidents are reported, investigated, responded to, and corrective action taken (including penalties)?	Is it standard business practice for suspected incidents to be reported, investigated, responded to, and corrective action taken (including penalties)?
6.4.1	Incident and Emergency Response	Continuity of Operations	Is a committee or project task force responsible for continuity of operations planning?	FISCAM SC-2; NIST SP 800-12 11.4.1	Is there a policy that requires a committee or project task force be responsible for continuity of operations planning?	Are there procedures for making a committee or project task force responsible for continuity of operations planning?	Is a committee or project task force responsible for continuity of operations planning?	Have periodic examinations been performed by an independent third party to verify that a committee or project task force is responsible for continuity of operations planning?	Is it standard business practice to make a committee or project task force responsible for continuity of operations planning?
6.4.2	Incident and Emergency Response	Continuity of Operations	Is there a business/mission continuity plan?	FISCAM SC-3; NIST SP 800-12 11.5	Is there a policy that requires a business/mission continuity plan?	Are there procedures for developing/maintaining a business/mission continuity plan?	Is there a business/mission continuity plan?	Has the business/mission continuity plan been tested as extensively as possible (in an operational versus simulated fashion)?	Is it standard business practice to develop and maintain a business/mission continuity plan?
6.4.3	Incident and Emergency Response	Continuity of Operations	Has a mission/business impact analysis been identified for continuity of operations planning?	FISCAM SC-1; FISCAM SC-2; NIST SP 800-18 5.MA.4; NIST SP 800-18 5.GSS.4; NIST SP 800-14 3.6.1; NIST SP 800-12	Is there a policy that requires identification of a mission/business impact analysis for continuity of operations planning?	Are there procedures for identification of a mission/business impact analysis for continuity of operations planning?	Has a mission/business impact analysis been identified for continuity of operations planning?	Have periodic examinations been performed by an independent third party to verify that a mission/business impact analysis has been identified for continuity of operations planning?	Is it standard business practice to identify a mission/business impact analysis for continuity of operations planning?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
6.4.4	Incident and Emergency Response	Continuity of Operations	Have emergency response and operations procedures been developed as part of continuity of operations planning?	FISCAM SC-3; NIST SP 800-18 5.MA.4; NIST SP 800-18 5.GSS.4; NIST SP 800-14 3.6.4	Is there a policy that requires development of emergency response and operations procedures as part of continuity of operations planning?	Are there procedures for development of emergency response and operations procedures as part of continuity of operations planning?	Have emergency response and operations procedures been developed as part of continuity of operations planning?	Have periodic examinations been performed by an independent third party to verify that emergency response and operations procedures have been developed as part of continuity of operations planning?	Is it standard business practice to develop emergency response and operations procedures as part of continuity of operations planning?
6.4.5	Incident and Emergency Response	Continuity of Operations	Have applicable procedures and policies been established to coordinate with public authorities for continuity of operations?	FISCAM SC-3	Is there a policy that requires establishment of applicable procedures and policies to coordinate with public authorities for continuity of operations?	Are there procedures for establishing applicable procedures and policies to coordinate with public authorities for continuity of operations?	Have applicable procedures and policies been established to coordinate with public authorities for continuity of operations?	Have periodic examinations been performed by an independent third party to verify that applicable procedures and policies have been established to coordinate with public authorities for continuity of operations?	Is it standard business practice to establish applicable procedures and policies to coordinate with public authorities for continuity of operations?
6.4.6	Incident and Emergency Response	Continuity of Operations	Have controls and safeguards to prevent or minimize the effect of the loss potential been identified for continuity of operations?	FISCAM SC-2; NIST SP 800-14 3.6.4	Is there a policy that requires identification of controls and safeguards to prevent or minimize the effect of the loss potential for continuity of operations?	Are there procedures for identifying controls and safeguards to prevent or minimize the effect of the loss potential for continuity of operations?	Have controls and safeguards to prevent or minimize the effect of the loss potential been identified for continuity of operations?	Have periodic examinations been performed by an independent third party to verify that controls and safeguards to prevent or minimize the effect of the loss potential have been identified for continuity of operations?	Is it standard business practice to identify controls and safeguards to prevent or minimize the effect of the loss potential for continuity of operations?
6.4.7	Incident and Emergency Response	Continuity of Operations	Has senior management been a part of continuity of operations planning?	NIST SP 800-14 3.6.1	Is there a policy that requires senior management to be a part of continuity of operations planning?	Are there procedures for making senior management a part of continuity of operations planning?	Has senior management been a part of continuity of operations planning?	Have periodic examinations been performed by an independent third party to verify that senior management is a part of continuity of operations planning?	Is it standard business practice to make senior management a part of continuity of operations planning?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
6.4.8	Incident and Emergency Response	Continuity of Operations	Have sufficient budget and resources been allocated for continuity of operations planning?	NIST SP 800-14 3.6.2; NIST SP 800-14 3.6.3; NIST SP 800-12 11.4.1	Is there a policy that requires sufficient budget and resources be allocated for continuity of operations planning?	Are there procedures for allocating sufficient budget and resources for continuity of operations planning?	Have sufficient budget and resources been allocated for continuity of operations planning?	Have periodic examinations been performed by an independent third party verify that sufficient budget and resources are allocated for continuity of operations planning?	Is it standard business practice to allocate sufficient budget and resources for continuity of operations planning?
6.4.9	Incident and Emergency Response	Continuity of Operations	Have individuals responsible for continuity of operations been identified and trained?	FISCAM SC-2.3; NIST SP 800-12 11.5.3; NIST SP 800-18 5.MA.5; NIST SP 800-18 5.GSS.4	Is there a policy that requires individuals responsible for continuity of operations be identified and trained?	Are there procedures for identifying and training individuals responsible for continuity of operations?	Have individuals responsible for continuity of operations been identified and trained?	Have periodic examinations been performed by an independent third party verify that individuals responsible for continuity of operations have been identified and trained?	Is it standard business practice to identify and train individuals responsible for continuity of operations?
6.4.10	Incident and Emergency Response	Continuity of Operations	Have interdependencies related to continuity of operations been identified and resolved?	NIST SP 800-12 11.7	Is there a policy that requires interdependencies related to continuity of operations be identified and resolved?	Are there procedures for identifying and resolving interdependencies related to continuity of operations?	Have interdependencies related to continuity of operations been identified and resolved?	Have periodic examinations been performed by an independent third party verify that interdependencies related to continuity of operations have been identified and resolved?	Is it standard business practice to identify and resolve interdependencies related to continuity of operations?
6.4.11	Incident and Emergency Response	Continuity of Operations	Have alternative sites and off-site storage been identified for continuity of operations?	FISCAM SC-2.1; FISCAM SC-3.2; NIST SP 800-12 11.4.2; NIST SP 800-18 5.MA.4; NIST SP 800-18 5.GSS.4	Is there a policy that requires identification of alternative sites and off-site storage for continuity of operations?	Are there procedures for identification of alternative sites and off-site storage for continuity of operations?	Have alternative sites and off-site storage been identified for continuity of operations?	Have periodic examinations been performed by an independent third party verify that alternative sites and off-site storage have been identified for continuity of operations?	Is it standard business practice to identify alternative sites and off-site storage for continuity of operations?
6.4.12	Incident and Emergency Response	Continuity of Operations	Have emergency telecommunications plans been established for continuity of operations?	FISCAM SC-3.2	Is there a policy that requires emergency telecommunications plans to be established for continuity of operations?	Are there procedures for establishing emergency telecommunications plans for continuity of operations?	Have emergency telecommunications plans been established for continuity of operations?	Have periodic examinations been performed by an independent third party verify that emergency telecommunications plans have been established for continuity of operations?	Is it standard business practice to establish emergency telecommunications plans for continuity of operations?
7.1.1	Operational Security Controls	HW and systems SW maintenance	Are official electronic records properly disposed/archived?	NIST SP 800-18; OMB Cir A-130 App III	Is there a policy that requires proper disposal and archival of official electronic records?	Are there procedures for proper disposal and archival of official electronic records?	Are official electronic records properly disposed/archived?	Are periodic third party reviews conducted to verify that all official electronic records are properly disposed/archived?	Is proper disposal and archival of official electronic records standard business practice?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
7.1.2	Operational Security Controls	HW and systems SW maintenance	Is information or media purged, overwritten, degaussed, or destroyed prior to disposal?	OMB Cir A-130 App III; NIST SP 800-18; FISCAM AC-3.4	Is there a policy that requires purging, overwriting, degaussing, or destroying information or media prior to disposal?	Are there procedures for purging, overwriting, degaussing, or destroying information or media prior to disposal?	Is information or media purged, overwritten, degaussed, or destroyed prior to disposal?	Are information or media that have been disposed of periodically examined to verify that they have been purged, overwritten, degaussed, or destroyed prior to disposal?	Is purging, overwriting, degaussing, or destroying information or media prior to disposal standard business practice?
7.1.3	Operational Security Controls	HW and systems SW maintenance	Is media sanitized prior to reuse?	NIST SP 800-18; FISCAM AC-3.4	Is there a policy that requires media sanitization prior to reuse?	Are there procedures for sanitizing media prior to reuse?	Is media sanitized prior to reuse?	Is reused media periodically examined to ensure sanitization prior to reuse?	Is sanitizing media prior to reuse standard business practice?
7.1.4	Operational Security Controls	HW and systems SW maintenance	Are the contents of damaged media stored and the media then destroyed?	NIST SP 800-18	Is there a policy that requires the contents of damaged media be stored and the media then destroyed?	Are there procedures for storing the contents of damaged media and then destroying the media?	Are the contents of damaged media stored and the media then destroyed?	Is all media periodically examined to ensure that the contents of damaged media are stored and the media then destroyed?	Is storing the contents of damaged media and then destroying the media standard business practice?
7.1.5	Operational Security Controls	HW and systems SW maintenance	Is hardcopy media shredded or destroyed when no longer needed?	NIST SP 800-18	Is there a policy that requires shredding or destroying hardcopy media when the media is no longer needed?	Are there procedures for shredding or destroying hardcopy media when the media is no longer needed?	Is hardcopy media shredded or destroyed when no longer needed?	Is hardcopy media that is no longer needed periodically examined to ensure shredding or destruction?	Is shredding or destroying hardcopy media when the media is no longer needed standard business practice?
7.1.6	Operational Security Controls	HW and systems SW maintenance	Do only authorized personnel handle the destruction of sensitive hardcopy media?	NIST SP 800-18	Is there a policy that requires only authorized personnel handle the destruction of sensitive hardcopy media?	Are there procedures for authorized personnel to destroy sensitive hardcopy media?	Do only authorized personnel handle the destruction of sensitive hardcopy media?	Are there periodic third party reviews to ensure only authorized personnel handle the destruction of sensitive hardcopy media?	Is it standard business practice for only authorized personnel to destroy sensitive hardcopy media?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
7.1.7	Operational Security Controls	HW and systems SW maintenance	Is access to system software (SW) and hardware (HW) (i.e., MA/AIS and GSS) appropriately controlled?	OMB Cir A-130 App III	Is there a policy that requires control of access to system software (SW) and hardware (HW) (i.e., MA/AIS and GSS)?	Are there procedures for controlling access to system software (SW) and hardware (HW) (i.e., MA/AIS and GSS)?	Is access to system software (SW) and hardware (HW) (i.e., MA/AIS and GSS) appropriately controlled?	Is access to system software (SW) and hardware (HW) (i.e., MA/AIS and GSS) periodically examined by an independent third party to verify appropriate controls are in place and functioning properly?	Is controlled access to system software (SW) and hardware (HW) (i.e., MA/AIS and GSS) standard business practice?
7.1.8	Operational Security Controls	HW and systems SW maintenance	Is virus detection and elimination software installed and activated?	OMB Cir A-130 App III	Is there a policy that requires virus detection and elimination software be installed and activated?	Are there procedures for installing and activating virus detection and elimination software?	Is virus detection and elimination software installed and activated?	Are all systems periodically examined to ensure that virus detection and elimination software is installed and activated?	Is installation and activation of virus detection and elimination software standard business practice on all systems?
7.2.1	Operational Security Controls	Data integrity	Is data confidentiality and integrity appropriately protected?	OMB Cir A-130 App III; FISCAM SP-1	Is there a policy that requires protections to ensure data confidentiality and integrity?	Are there procedures for applying protections to ensure data confidentiality and integrity?	Is data confidentiality and integrity appropriately protected?	Are data confidentiality and integrity requirements periodically assessed and protections examined to ensure appropriate protection?	Is applying adequate protections to ensure data confidentiality and integrity standard business practice?
7.2.2	Operational Security Controls	Data integrity	Are the planned and in-place controls consistent with the identified risks and the system and data integrity?	OMB Cir A-130 App III; NIST SP 800-18	Is there a policy that requires planned and in-place controls be consistent with the identified risks and the system and data integrity?	Are there procedures for identifying and implementing controls that are consistent with the identified risks and the system and data integrity?	Are the planned and in-place controls consistent with the identified risks and the system and data integrity?	Are the planned and in-place controls periodically verified by an independent third part to ensure consistency with the identified risks and the system and data integrity?	Is identifying and implementing controls that are consistent with the identified risks and the system and data integrity part of the standard business practice?
7.2.3	Operational Security Controls	Data integrity	Are critical data files identified and the frequency of file backup documented?	NIST SP 800-18; FISCAM SC-1.1; FISCAM SC-3.1	Is there a policy that requires that critical data files be identified and the frequency of file backup documented?	Are there procedures for identifying critical data files and documenting the frequency of file backup?	Are critical data files identified and the frequency of file backup documented?	Are identification of critical data files and the documentation of file backup frequency periodically verified by an independent third party?	Is identifying critical data files and documenting the frequency of file backups part of the standard business practice?
7.2.4	Operational Security Controls	Data integrity	Are default settings of security features set to the most restrictive mode?	NIST SP 800-18	Is there a policy that requires default settings of security features be set to the most restrictive mode?	Are there procedures for setting default settings of security features to the most restrictive mode?	Are default settings of security features reset to the most restrictive mode?	Are default settings of security features periodically verified to be reset to the most restrictive mode by an independent third party?	Is setting the security features to the most restrictive mode part of the standard business practice?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
7.2.5	Operational Security Controls	Data integrity	Are virus signature files routinely updated?	NIST SP 800-18	Is there a policy that requires that virus signature files be routinely updated?	Are there procedures for routinely updating virus signature files?	Are virus signature files routinely updated?	Does an independent third party on a periodic basis verify the routine updating of virus signature files?	Is the routine updating of virus signature files part of the standard business process?
7.2.6	Operational Security Controls	Data integrity	Are virus scans automatic?	NIST SP 800-18	Is there a policy that requires automatic virus scans?	Are there procedures for automating virus scans?	Are virus scans automatic?	Is the automatic scanning for viruses verified periodically by an independent third party?	Is the automatic scanning for virus part of the standard business process?
7.2.7	Operational Security Controls	Data integrity	Are data integrity and validation controls used to provide assurance that the information has not been altered and the system functions as intended?	FISCAM CC-2.1	Is there a policy that requires that data integrity and validation controls be used to provide assurance that the information has not been altered and that the system functions as intended?	Are there procedures for using data integrity and validation controls to provide assurance that the information has not been altered and that the system functions as intended?	Are data integrity and validation controls used to provide assurance that the information has not been altered and the system functions as intended?	Does an independent third party verify the use of data integrity and validation controls to provide assurance that the information has not been altered and that the system functions as intended periodically?	Is the use of data integrity and validation controls to provide assurance that the information has not been altered and that the system functions as intended a part of the standard business process?
7.2.8	Operational Security Controls	Data integrity	Are reconciliation routines used by applications, i.e., checksums, hash totals, and record counts?	NIST SP 800-18	Is there a policy that requires reconciliation routines be used by applications (i.e., checksums, hash totals, and record counts)?	Are there procedures for the use of reconciliation routines by applications (i.e., checksums, hash totals, record counts)?	Are reconciliation routines used by applications, i.e., checksums, hash totals, and record counts?	Is the use of reconciliation routines by applications periodically verified by an independent third party?	Is the use of reconciliation routines by applications a part of the standard business process?
7.2.9	Operational Security Controls	Data integrity	Are integrity verification programs used by applications to look for evidence of data tampering, errors, and omissions?	NIST SP 800-18	Is there a policy that requires integrity verification programs be used by applications to look for evidence of data tampering, errors, and omissions?	Are there procedures for using integrity verification programs by applications to look for evidence of data tampering, errors, and omissions?	Are integrity verification programs used by applications to look for evidence of data tampering, errors, and omissions?	Is the use of integrity verification programs by applications periodically verified by an independent third party?	Is the use of integrity verification programs by applications a part of the standard business process?
7.2.10	Operational Security Controls	Data integrity	Are intrusion detection tools installed on the system?	NIST SP 800-18	Is there a policy that requires intrusion detection tools be installed on the system?	Are there procedures for intrusion detection tools being installed on the system?	Are intrusion detection tools installed on the system?	Is the installation of intrusion detection tools on the system periodically verified by an independent third party?	Is the installation of intrusion detection tools on the system a part of the standard business process?
7.2.11	Operational Security Controls	Data integrity	Is system performance monitoring used to analyze system performance logs in real time to look for availability problems, including active attacks?	NIST SP 800-18	Is there a policy that requires system performance monitoring to analyze system performance logs in real time to look for availability problems, including active attacks?	Are there procedures for using system performance monitoring to analyze system performance logs in real time to look for availability problems, including active attacks?	Is system performance monitoring used to analyze system performance logs in real time to look for availability problems, including active attacks?	Is the use of system performance monitoring tools to analyze system performance logs in real time to look for availability problems periodically verified by an independent third party?	Is the use of system performance monitoring to analyze system performance logs in real time a part of the standard business process?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
7.2.12	Operational Security Controls	Data integrity	Is message authentication used in applications to ensure that the sender of a message is known and that the message has not been altered?	NIST SP 800-18	Is there a policy that requires message authentication be used in applications to ensure that the sender of a message is known and that the message has not been altered?	Are there procedures for message authentication use in applications to ensure that the sender of a message is known and that the message has not been altered?	Is message authentication used in applications to ensure that the sender of a message is known and that the message has not been altered?	Is message authentication use in applications to ensure that the sender of a message is known and that the message has not been altered periodically verified by an independent third party?	Is the use of message authentication in applications to ensure that the sender of a message is known and that the message has not been altered a part of the standard business process?
7.2.13	Operational Security Controls	Data integrity	Are passwords transmitted and stored using secure protocols/algorithms?	NIST SP 800-18; FISCAM AC-3.2	Is there a policy that requires that passwords be transmitted and stored using secure protocols/algorithms?	Are there procedures for using secure protocols/algorithms for password transmission and storage?	Are passwords transmitted and stored using secure protocols/algorithms?	Is password transmission and storage using secure protocols/algorithms periodically verified by an independent third party?	Is the use of secure protocols/algorithms for transmitting and storing passwords a part of the standard business process?
7.2.14	Operational Security Controls	Data integrity	If encryption is used, does it meet federal standards?	NIST SP 800-18	Is there a policy that requires that encryption meet federal standards if it is used?	Are there procedures requiring that if encryption is used, it must meet federal standards?	If encryption is used, does it meet federal standards?	Does an independent third party verify the meeting of federal standards for any encryption used periodically?	Is the meeting of federal standards for encryption products a part of the standard business process?
7.2.15	Operational Security Controls	Data integrity	If encryption is used, are there procedures for key generation, distribution, storage, use, destruction, and archiving?	NIST SP 800-18	Is there a policy that requires that procedures be in place for key generation, distribution, storage, use, destruction, and archiving for any encryption in use?	Are there procedures in place for key generation, distribution, storage, use, destruction, and archiving for any encryption used?	If encryption is used, are there procedures for key generation, distribution, storage, use, destruction, and archiving?	Is the existence of procedures for key generation, distribution, storage, use, destruction, and archiving for any encryption used periodically verified by an independent third party?	If encryption is used, are there procedures for key generation, distribution, storage, use, destruction, and archiving?
7.2.16	Operational Security Controls	Data integrity	Have all vendor-supplied default security parameters been reinitialized to more secure settings?	NIST SP 800-18	Is there a policy that requires that all vendor-supplied default security parameters be reinitialized to more secure settings?	Are there procedures requiring that all vendor-supplied default security parameters be reinitialized to more secure settings?	Have all vendor-supplied default security parameters been reinitialized too more secure settings?	Is the reinitialization of vendor-supplied default security parameters to more secure settings periodically verified by an independent third party?	Is having vendor-supplied default security settings reinitialized to more secure settings part of the standard business process?
7.2.17	Operational Security Controls	Data integrity	If the public accesses the system, are there controls implemented to protect the integrity of the application and the confidence of the public?	NIST SP 800-18	Is there a policy for systems accessed by the public that controls be implemented to protect the integrity of the application and the confidence of the public?	Are there procedures for systems accessed by the public that requires controls be implemented to protect the integrity of the application and the confidence of the public?	If the public accesses the system, are there controls implemented to protect the integrity of the application and the confidence of the public?	Is the implementation of controls for systems accessed by the public to protect the integrity of the application and the confidence of the public periodically verified by an independent third party?	Is the implementation of controls for public-accessed systems to protect the integrity of the application and the confidence of the public part of the standard business process?
7.2.18	Operational Security Controls	Data integrity	Are off-line storage of audit logs retained for a period of time, and if so, is access to audit logs strictly controlled?	NIST SP 800-18	Is there a policy requiring off-line storage and strictly controlled access of audit logs retained for a period of time?	Are there procedures for off-line storage of audit logs, and strict access control to those audit logs?	Are off-line storage of audit logs retained for a period of time, and if so, is access to audit logs strictly controlled?	Is off-line storage and strict access control for audit logs retained for a period of time periodically verified by an independent third party?	Is off-line storage and strict access control for audit logs a part of the standard business process?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
7.2.19	Operational Security Controls	Data integrity	Are reconciliation routines used by the system, (i.e., checksums, hash totals, record counts) to ensure the integrity of critical data?	NIST SP 800-18	Is there a policy requiring that reconciliation routines be used to ensure the integrity of critical data?	Are there procedures that describe the use of reconciliation routines by the system to ensure the integrity of critical data?	Are reconciliation routines used by the system, (i.e., checksums, hash totals, record counts) to ensure the integrity of critical data?	Is the use of reconciliation routines by the system to ensure the integrity of critical data periodically verified by an independent third party?	Is the use of reconciliation routines by the system to ensure the integrity of critical data part of the normal business process?
7.2.20	Operational Security Controls	Data integrity	Are integrity verification programs used by applications to look for evidence of data tampering, errors, and omissions on critical system?	NIST SP 800-18	Is there a policy requiring the use of integrity verification programs by applications to look for evidence of data tampering, errors, or omissions on critical systems?	Are there procedures for using integrity verification programs by applications to look for evidence of data tampering, errors, or omissions on critical systems?	Are integrity verification programs used by applications to look for evidence of data tampering, errors, and omissions on critical system?	Is the use of integrity verification programs by applications to look for evidence of data tampering, errors, or omissions on critical systems periodically verified by an independent third party?	Is the use of integrity verification programs by applications to look for evidence of data tampering, errors, or omissions on critical systems part of the normal business process?
7.2.21	Operational Security Controls	Data integrity	Is secret key cryptography used to calculate a message authentication code (MAC) from and appended to critical data to ensure its integrity.	NIST SP 800-12	Is there a policy that requires that secret key cryptography be used to calculate a message authentication code from and appended to critical data to ensure its integrity?	Are there procedures defining the process for implementing secret key cryptography to calculate a message authentication code from and appended to critical data to ensure its integrity?	Is secret key cryptography used to calculate a message authentication code (MAC) from and appended to critical data to ensure its integrity?	Is the use of secret key cryptography to calculate a message authentication code from and appended to critical data to ensure its integrity periodically verified by an independent third party?	Is the use of secret key cryptography to calculate a message authentication code from and appended to critical data to ensure its integrity part of the normal business process?
7.3.1	Operational Security Controls	Production I/O	Is there user support?	NIST SP 800-18	Is there a policy requiring user support?	Are there procedures for providing user support?	Is there user support?	Is user support periodically examined and verified by an independent third party?	Is providing user support a part of the normal business process?
7.3.2	Operational Security Controls	Production I/O	Is there a help desk or group that offers advice?	NIST SP 800-18	Is there a policy requiring a help desk or a group that offers advice?	Are there procedures that define the operation of a help desk or a group that offers advice?	Is there a help desk or group that offers advice?	Is the help desk or user support group periodically examined by an independent third party?	Is providing help desk or group offering advice a part of the normal business process?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
7.3.3	Operational Security Controls	Production I/O	Are there media controls?	NIST SP 800-18	Is there a policy covering media controls?	Are there procedures for media controls?	Are there media controls?	Are media controls periodically verified by an independent third party?	Is media controls part of the normal business process?
7.3.4	Operational Security Controls	Production I/O	Controls ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information?	NIST SP 800-18	Is there a policy requiring that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information?	Are there procedures for ensuring that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information?	Are unauthorized individuals unable to read, copy, alter, or steal printed or electronic information?	Are there periodic verifications by an independent third party that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information?	Is ensuring that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information part of the normal business process?
7.3.5	Operational Security Controls	Production I/O	Can only authorized users pick up, receive, or deliver input and output information and media?	NIST SP 800-18	Is there a policy requiring that only authorized users may pick up, receive, or deliver input and output information and media?	Are there procedures for ensuring that only authorized users pick up, receive, or deliver input and output information and media?	Are only authorized users able to pick up, receive, or deliver input and output information and media?	Are there periodic verifications by an independent third party that only authorized users may pick up, receive, or deliver input and output information and media?	Are controls ensuring that only authorized users may pick up, receive, or deliver input and output information and media part of the normal business process?
7.3.6	Operational Security Controls	Production I/O	Is there internal/external labeling of media for sensitivity?	NIST SP 800-18	Is there a policy that requires internal/external labeling of media for sensitivity?	Are there procedures for internal/external labeling of media for sensitivity?	Is there internal/external labeling of media for sensitivity?	Does an independent third party verify internal/external labeling of media for sensitivity periodically?	Is internal/external labeling of media for sensitivity a part of the normal business process?
7.3.7	Operational Security Controls	Production I/O	Is media given external labeling with special handling instructions?	NIST SP 800-18	Is there a policy that requires media be given external labeling with special handling instructions?	Are there procedures for external labeling of media including special handling instructions?	Is media given external labeling with special handling instructions?	Does an independent third party periodically verify external labeling and special handling instructions for media?	Is the use of external labeling and special handling instructions for media a part of the normal business process?
7.3.8	Operational Security Controls	Production I/O	Have processing priorities been established and approved by management?	FISCAM SC-1.3	Is there a policy requiring that processing priorities be established and approved by management?	Are there procedures for establishing and approving of processing priorities by management?	Have processing priorities been established and approved by management?	Is processing priority establishment and approval by management periodically verified by an independent third party?	Is the establishment and approval of processing priorities by management a part of the normal business process?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
7.3.9	Operational Security Controls	Production I/O	Is penetration testing performed on the system?	NIST SP 800-18	Is there a policy covering penetration testing on the system?	Are there procedures covering penetration testing of the system?	Is penetration testing performed on the system?	Is penetration testing of the system periodically verified by an independent third party?	Is penetration testing of the system a part of the normal business process?
7.3.10	Operational Security Controls	Production I/O	Are there written agreements regarding how data is shared between interconnected systems?	NIST SP 800-18; OMB Cir A-130 App III	Is there a policy requiring written agreements regarding how data is shared between interconnected systems?	Are there procedures covering written agreements regarding how data is shared between interconnected systems?	Are there written agreements regarding how data is shared between interconnected systems?	Are written agreements regarding data sharing between interconnected systems periodically verified by an independent third party?	Are written agreements regarding data sharing between interconnected systems part of the normal business process?
7.3.11	Operational Security Controls	Production I/O	Do secure gateways limit access between telecommunications and critical systems?	FISCAM AC-3.2	Is there a policy requiring secure gateways to restrict access between telecommunications systems and critical systems?	Are there procedures requiring secure gateways between telecommunications systems and critical systems to limit access?	Do secure gateways limit access between telecommunications and critical systems?	Are secure gateways between telecommunications and critical system to limit access periodically reviewed by an independent third party?	Are the use of secure gateways to limit access between telecommunications systems and critical systems a part of the normal business process?
7.3.12	Operational Security Controls	Production I/O	Is dialup access to critical systems documented and approved by system owners?	FISCAM AC-2.1	Is there a policy requiring that dialup access to critical systems be documented and approved by system owners?	Are there procedures for documentation and approval by system owners of dialup access to critical systems?	Is dialup access to critical systems documented and approved by system owners?	Is the documentation and approval of dialup access to critical systems by system owners periodically verified by an independent third party?	Is the documentation and approval of dialup access to critical systems by system owners part of the normal business process?
7.3.13	Operational Security Controls	Production I/O	Are dialback procedures to pre-authorized phone numbers used for dialup access to critical systems?	FISCAM AC-2.1	Is there a policy requiring that dialup access to critical systems use dial-back procedures to pre-authorized phone numbers?	Are there procedures covering dialbacks to pre-authorized phone numbers for dialup access to critical systems?	Are dialback procedures to pre-authorized phone numbers used for dialup access to critical systems?	Does an independent third party verify dialup access to critical systems using dialback procedures to pre-authorized phone numbers periodically?	Is dialup access to critical systems using dialback procedures to pre-authorized phone numbers part of the normal business process?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
7.3.14	Operational Security Controls	Production I/O	Are security modems, tokens, or smart cards used to authenticate a valid user accessing critical systems vial dial-up?	FISCAM AC-2.1	Is there a policy requiring that dialup access to critical systems use security modems, tokens, or smart cards to authenticate valid users?	Are there procedures for dialup access to critical systems using security modems, tokens, or smart cards to authenticate valid users?	Are security modems, tokens, or smart cards used to authenticate a valid user accessing critical systems vial dial-up?	Is the authentication of valid users accessing critical systems via dialup using security modems, tokens, or smart cards periodically verified by an independent third party?	Is the authentication of valid users accessing critical systems via dialup using security modems, tokens, or smart cards part of the normal business process?
7.3.15	Operational Security Controls	Production I/O	Are dialup connections automatically disconnected at the end of a session?	FISCAM AC-3.2	Is there a policy requiring automatic disconnection of dialup connections at the end of a session?	Are there procedures in place that cover the automatic disconnection of dialup connections at the end of a session?	Are dialup connections automatically disconnected at the end of a session?	Is the automatic disconnection of dialup connections at the end of a session periodically verified by an independent third party?	Is the automatic disconnection of dialup connections at the end of a session part of the normal business process?
7.4.1	Operational Security Controls	Data Confidentiality	Has data confidentiality been addressed in security plans, concepts of operations documents, disaster recovery procedures, or backup procedures for critical data?	NIST SP 800-18; OMB Cir A-130 App III	Is there a policy requiring that data confidentiality be addressed in security plans, concepts of operations documents, disaster recovery procedures, and backup procedures for critical data?	Are procedures in place that describe how data confidentiality be addressed in security plans, concepts of operations documents, disaster recovery procedures, and backup procedures for critical data?	Has data confidentiality been addressed in security plans, concepts of operations documents, disaster recovery procedures, or backup procedures for critical data?	Does an independent third party verify addressing data confidentiality in security plans, concepts of operations documents, disaster recovery procedures, and backup procedures for critical data periodically?	Is addressing data confidentiality in security plans, concepts of operations documents, disaster recovery procedures, and backup procedures for critical data part of the normal business process?
7.4.2	Operational Security Controls	Data Confidentiality	Has data confidentiality been taken into consideration for stored critical data? (Either online or offline [hard disks, tape cartridges, CD-ROMS?])	NIST SP 800-18; OMB Cir A-130 App III	Is there a policy requiring that data confidentiality be taken into consideration for stored critical data?	Are there procedures that detail the process for ensuring the confidentiality of stored critical data?	Has data confidentiality been taken into consideration for stored critical data? (Either online or offline [hard disks, tape cartridges, CD-ROMS?])	Is data confidentiality consideration for stored critical data periodically verified by an independent third party?	Is taking data confidentiality into consideration for stored critical data part of the normal business process?
7.4.3	Operational Security Controls	Data Confidentiality	Has data confidentiality been addressed for critical data that is transmitted either internally or externally (networks, modems, wired or wireless)?	NIST SP 800-18; OMB Cir A-130 App III	Is there a policy requiring that data confidentiality be ensured during the transmission of critical data?	Are there procedures that detail the process of ensuring the confidentiality of critical data during transmission?	Has data confidentiality been addressed for critical data that is transmitted either internally or externally (networks, modems, wired or wireless)?	Is data confidentiality for critical data being transmitted periodically verified by an independent third party?	Is providing data confidentiality for critical data during transmission part of the normal business process?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
7.5.1	Operational Security Controls	Data Availability	Is volume mirroring or RAID implementation used to ensure data availability for critical files?	NIST SP 800-18	Is there a policy requiring that volume mirroring or RAID implementation be used to ensure data availability for critical files?	Are there procedures for the implementation of volume mirroring or RAID implementation to ensure data availability for critical files?	Is volume mirroring or RAID implementation used to ensure data availability for critical files?	Is the use of volume mirroring or RAID implementation to ensure data availability of critical files periodically verified by an independent third party?	Is the use of volume mirroring or RAID implementation to ensure data availability of critical files part of the normal business process?
7.5.2	Operational Security Controls	Data Availability	Is system performance monitoring used to analyze system performance logs in real time to look for data availability problems?	NIST SP 800-18	Is there a policy requiring system performance monitoring to analyze system performance logs in real time to look for data availability problems?	Are there procedures for system performance monitoring to analyze system performance logs in real time to look for data availability problems?	Is system performance monitoring used to analyze system performance logs in real time to look for data availability problems?	Is the use of system performance monitoring tools to analyze system performance logs in real time to look for data availability problems periodically verified by an independent third party?	Is the use of system performance monitoring to analyze system performance logs in real time to look for data availability problems a part of the standard business process?
7.5.3	Operational Security Controls	Data Availability	Has the flow of critical data in the system been analyzed to identify critical-points-of-failure which were mediated?	FISCAM SC-1.1	Is there a policy requiring analysis of critical data flow to identify critical-points-of-failure and that they be mediated?	Are there procedures for analyzing flow of critical data to identify critical-points-of-failure and remediation of them?	Has the flow of critical data in the system been analyzed to identify critical-points-of-failure which were mediated?	Is the analysis of critical data flow to identify critical-points-of-failure for remediation periodically verified by an independent third party?	Is the analysis of critical data flow to identify critical-points-of-failure for remediation a part of the standard business process?
7.6.1	Operational Security Controls	Systems Operations Documentation	Is operating documentation updated when a new or modified system is implemented?	FISCAM CC-2.1	Is there a policy requiring operating documentation be updated when a new or modified system is implemented?	Are there procedures for updating operating documentation whenever a new or modified system is implemented?	Is operating documentation updated when a new or modified system is implemented?	Is the updating of operating documentation when a new or modified system is implemented periodically verified by an independent third party?	Is the updating of operating documentation when a new or modified system is implemented a part of the normal business process?
7.6.2	Operational Security Controls	Systems Operations Documentation	Does all system software have current and complete documentation?	FISCAM SS-3.2	Is there a policy requiring that all system software have current and complete documentation?	Are there procedures in place to ensure that all system software has current and complete documentation?	Does all system software have current and complete documentation?	Is the availability of current and complete documentation for the system software periodically verified by an independent third party?	Is having current and complete documentation for the system software part of the normal business process?
7.6.3	Operational Security Controls	Systems Operations Documentation	Is access to operating system documentation restricted to authorized systems personnel?	FISCAM SD-1.1	Is there a policy requiring that access to operating system documentation be restricted to authorized systems personnel?	Are there procedures for restricting access to operating system documentation to authorized personnel?	Is access to operating system documentation restricted to authorized systems personnel?	Is restricting access to operating system documentation to authorized systems personnel periodically verified by an independent third party?	Is restricting access to operating system documentation to authorized systems personnel part of the normal business process?
7.6.4	Operational Security Controls	Systems Operations Documentation	Is access to application system documentation restricted to authorized personnel?	FISCAM SD-1.1	Is there a policy requiring that access to application system documentation be restricted to authorized personnel?	Are there procedures for restricting access to application system documentation to authorized personnel?	Is access to application system documentation restricted to authorized personnel?	Is the restricting of access to application system documentation to authorized personnel periodically verified by an independent third party?	Is the restricting of access to application system documentation to authorized personnel part of the normal business process?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
7.6.5	Operational Security Controls	Systems Operations Documentation	Have critical operations and data been documented?	FISCAM SC-1.1	Is there a policy requiring that critical operations and data be documented?	Are there procedures for the identification and documentation of critical operations and data?	Have critical operations and data been documented?	Is the documentation of critical operations and data periodically verified by an independent third party?	Is the documentation of critical applications and data part of the normal business process?
7.6.6	Operational Security Controls	Systems Operations Documentation	Have resources supporting critical operations been documented?	FISCAM SC-1.1	Is there a policy requiring that resources supporting critical operations be documented?	Are there procedures for the documentation of resources supporting critical operations?	Have resources supporting critical operations been documented?	Is the documentation of resources supporting critical operations periodically verified by an independent third party?	Is the documentation of resources supporting critical operations part of the normal business process?
7.6.7	Operational Security Controls	Systems Operations Documentation	Are emergency processing priorities documented?	FISCAM SC-1.1	Is there a policy requiring that emergency processing priorities be documented?	Are there procedures for the documentation of emergency processing priorities?	Are emergency processing priorities documented?	Is the documentation of emergency processing priorities periodically verified by an independent third party?	Is the documentation of emergency processing priorities part of the normal business process?
7.6.8	Operational Security Controls	Systems Operations Documentation	Are system and application documentation maintained at an off-site storage location?	FISCAM SC-2.1	Is there a policy requiring that system and application documentation be maintained at an off-site storage location?	Are there procedures for the maintenance of system and application documentation at an off-site storage location?	Are system and application documentation maintained at an off site storage location?	Is the maintenance of system and application documentation at an off-site storage location periodically verified by an independent third party?	Is the maintenance of system and application documentation at an off-site storage location part of the normal business process?
8.1.1	Physical Security	Implementation of physical security controls	Have physical security controls commensurate with the risks of physical damage or access been identified?	NIST SP 800-18	Is there a policy that requires identification of physical security controls that are commensurate with the risks of physical damage or access?	Are there procedures for identification of physical security controls that are commensurate with the risks of physical damage or access?	Have physical security controls commensurate with the risks of physical damage or access been identified?	Has the process to identify physical security controls commensurate with the risks of physical damage or access been verified? Have the identified physical security controls been verified against current risks?	Is the identification of physical security controls commensurate with the risks of physical damage or access integrated into the system development and maintenance process?
8.1.2	Physical Security	Implementation of physical security controls	Is access to facilities controlled through the use of guards, identification badges, or entry devices such as key cards?	NIST SP 800-18; FISCAM AC-3	Is there a policy that requires control of access to facilities through the use of guards, identification badges, or entry devices such as key cards?	Are there procedures for controlling access to facilities through the use of guards, identification badges, or entry devices such as key cards?	Is access to facilities controlled through the use of guards, identification badges, or entry devices such as key cards?	Is access to facilities periodically tested by an independent third party to ensure appropriate controlled access through the use of guards, identification badges, or entry devices such as key cards?	Is controlled facility access a standard part of doing business?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
8.1.3	Physical Security	Implementation of physical security controls	Does management regularly review the list of persons with physical access to sensitive facilities?	FISCAM AC-3.1	Is there a policy that requires regular management review of the list of persons with physical access to sensitive facilities? Is the periodicity of review specified?	Are there procedures for regular management review of the list of persons with physical access to sensitive facilities?	Does management regularly review the list of persons with physical access to sensitive facilities?	Is the management review of the list of persons with physical access to sensitive facilities periodically verified by an independent third party?	Is a regular management review of the list of persons with physical access to sensitive facilities an integrated part of the business process? Is it performed and accepted without question?
8.1.4	Physical Security	Implementation of physical security controls	Are deposits and withdrawals of tapes and other storage media from the library authorized and logged?	FISCAM AC-3.1	Is there a policy that requires authorizing and logging of deposits and withdrawals of tapes and other storage media from the library? Are authorizing officials identified?	Are there procedures for authorizing and logging deposits and withdrawals of tapes and other storage media from the library?	Are deposits and withdrawals of tapes and other storage media from the library authorized and logged?	Are deposits and withdrawals of tapes and other storage media from the library periodically reviewed to ensure adequate controls are in place?	Is it standard business practice to authorize and log all deposits and withdrawals of tapes and other storage media from the library?
8.1.5	Physical Security	Implementation of physical security controls	Are unused keys and other entry devices secured?	FISCAM AC-3.1	Is there a policy that requires unused keys and other entry devices to be secured?	Are there procedures for securing unused keys and other entry devices?	Are unused keys and other entry devices secured?	Are periodic inspections performed to ensure that unused keys and other entry devices are secured?	Is it standard business practice to secure unused keys and other entry devices?
8.1.6	Physical Security	Implementation of physical security controls	Do emergency exit and re-entry procedures ensure that only authorized personnel are allowed to re-enter after fire drills or other emergency exits?	FISCAM AC-3.1	Is there a policy that requires implementation of sufficient procedures to ensure only authorized personnel are allowed to re-enter after fire drills or other emergency exits?	Are there procedures for implementation of sufficient procedures to ensure only authorized personnel are allowed to re-enter after fire drills or other emergency exits?	Do emergency exit and re-entry procedures ensure that only authorized personnel are allowed to re-enter after fire drills or other emergency exits?	Are emergency exits and re-entries tested to verify that only authorized personnel are allowed to re-enter after fire drills or other emergency exits?	Is it standard business practice to ensure only authorized personnel are allowed to re-enter after fire drills or other emergency exits?
8.1.7	Physical Security	Implementation of physical security controls	Are all visitors to sensitive areas signed in, badged, and if appropriate, escorted?	FISCAM AC-3.1	Is there a policy that requires all visitors to sensitive areas be signed in and badged? If appropriate, does the policy define under what circumstances visitors must be escorted?	Are there procedures for signing in and badging all visitors to sensitive areas? If appropriate, are there procedures for escorting visitors?	Are all visitors to sensitive areas signed in, badged, and if appropriate, escorted?	Are periodic inspections performed to verify that all visitors to sensitive areas are signed in, badged, and if appropriate, escorted?	Is it standard business practice to sign in and badge all visitors to sensitive areas and if appropriate, escort them for the duration of their visit?
8.1.8	Physical Security	Implementation of physical security controls	Are entry codes changed periodically?	FISCAM AC-3.1	Is there a policy that requires all entry codes to be changed periodically? Is the periodicity defined for entry to different locales (e.g. facility, computer room, network closet, phone closet)?	Are there procedures for changing all entry codes (e.g. facility, computer room, network closet, phone closet)?	Are entry codes changed periodically?	Are there periodic reviews to verify that entry codes are changed periodically?	Is it standard business practice to change entry codes periodically?
8.1.9	Physical Security	Implementation of physical security controls	Are physical accesses monitored through audit trails and apparent security violations investigated and remedial action taken?	FISCAM AC-4	Is there a policy that requires monitoring of physical accesses through audit trails and investigation of apparent security violations? Does the policy require that remedial action be taken?	Are there procedures for monitoring physical accesses through audit trails and investigation of apparent security violations? Are there procedures for taking remedial action?	Are physical accesses monitored through audit trails and apparent security violations investigated and remedial action taken?	Is there a periodic independent third party validation that physical accesses are monitored through audit trails and apparent security violations investigated and remedial action taken?	Is it standard business practice to monitor physical accesses through audit trails, investigate apparent security violations, and take remedial action?
8.1.10	Physical Security	Implementation of physical security controls	Is suspicious physical access activity investigated and appropriate action taken?	FISCAM AC-4.3	Is there a policy that requires investigation of suspicious physical access activity? Does the policy require and specify appropriate action?	Are there procedures for investigation of suspicious physical access activity? Are there procedures for taking appropriate action?	Is suspicious physical access activity investigated and appropriate action taken?	Is there a periodic validation by an independent third party that suspicious physical access activity is investigated and appropriate action taken?	Is it standard business practice to investigate suspicious physical access activity and take appropriate action?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
8.1.11	Physical Security	Implementation of physical security controls	Are visitors, contractors, and maintenance personnel authenticated through the use of pre-planned appointments and identification checks?	FISCAM AC-3.1	Is there a policy that requires visitors, contractors, and maintenance personnel be authenticated through the use of pre-planned appointments and identification checks?	Are there procedures for authenticating visitors, contractors, and maintenance personnel through the use of pre-planned appointments and identification checks?	Are visitors, contractors, and maintenance personnel authenticated through the use of pre-planned appointments and identification checks?	Is the authentication of visitors, contractors, and maintenance personnel through the use of pre-planned appointments and identification checks periodically validated by an independent third party?	Is the authentication of visitors, contractors, and maintenance personnel through the use of pre-planned appointments and identification checks standard business practice?
8.1.12	Physical Security	Implementation of physical security controls	Are appropriate fire suppression and prevention devices installed and working?	NIST SP 800-18; FISCAM SC-2.2	Is there a policy that requires appropriate fire suppression and prevention devices be installed and working?	Are there procedures for installing appropriate fire suppression and prevention devices?	Are appropriate fire suppression and prevention devices installed and working?	Are fire suppression and prevention devices periodically examined to ensure the devices are appropriate for the circumstances and that they are in complete working order?	Is installation and maintenance of appropriate and working fire suppression and prevention devices periodically standard business practice?
8.1.13	Physical Security	Implementation of physical security controls	Are sources of fire ignition, such as failure of electronic devices or wiring, improper storage materials, and the possibility of arson, thoroughly examined and mitigated against?	NIST SP 800-18	Is there a policy that requires periodic examination and mitigation against sources of fire ignition, such as failure of electronic devices or wiring, improper storage materials? Is the periodicity defined?	Are there procedures for periodic examination and mitigation against sources of fire ignition, such as failure of electronic devices or wiring, improper storage materials?	Are sources of fire ignition, such as failure of electronic devices or wiring, improper storage materials, and the possibility of arson, thoroughly examined and mitigated against?	Are sources of fire ignition, such as failure of electronic devices or wiring, improper storage materials, and the possibility of arson, periodically reviewed by an independent third party to ensure proper identification? Are the mitigation measures also reviewed for appropriateness?	Is the identification of and mitigation against sources of fire ignition, such as failure of electronic devices or wiring, improper storage materials, standard business practice?
8.1.14	Physical Security	Implementation of physical security controls	Are heating and air-conditioning systems in proper working order?	NIST SP 800-18	Is there a policy that requires heating and air-conditioning systems to be in proper working order?	Are there procedures for periodic maintenance of heating and air-conditioning systems?	Are heating and air-conditioning systems in proper working order?	Are heating and air-conditioning systems periodically tested to verify that they are in proper working order?	Are appropriately functioning heating and air-conditioning systems a standard part of the business environment?
8.1.15	Physical Security	Implementation of physical security controls	Are there redundant air-cooling systems?	FISCAM SC-2.2	Is there a policy that requires redundant air-cooling systems?	Are there procedures for providing redundant air-cooling systems?	Are there redundant air-cooling systems?	Are the redundant air-cooling systems periodically tested to ensure proper functioning?	Are redundant air-cooling systems a standard part of the business environment?
8.1.16	Physical Security	Implementation of physical security controls	Are electric power distribution, heating plants, water, sewage, and other utilities in proper working order?	NIST SP 800-18; FISCAM SC-2.2	Is there a policy that requires electric power distribution, heating plants, water, sewage, and other utilities to be in proper working order?	Are there procedures for periodic maintenance of electric power distribution, heating plants, water, sewage, and other utilities?	Are electric power distribution, heating plants, water, sewage, and other utilities in proper working order?	Are electric power distribution, heating plants, water, sewage, and other utilities periodically tested to verify that they are in proper working order?	Are appropriately functioning electric power distribution, heating plants, water, sewage, and other utilities a standard part of the business environment?
8.1.17	Physical Security	Implementation of physical security controls	Are systems located so that leaks in the plumbing do not endanger the systems?	NIST SP 800-18; FISCAM SC-2.2	Is there a policy that requires systems to be located so that leaks in the plumbing do not endanger the systems?	Are there procedures for locating systems so that leaks in the plumbing do not endanger the systems?	Are systems located so that leaks in the plumbing do not endanger the systems?	Are system locations periodically reviewed to ensure that leaks in the plumbing do not endanger the systems?	Is it standard business practice to locate systems so that leaks in the plumbing do not endanger the systems?
8.1.18	Physical Security	Implementation of physical security controls	Is a backup power supply in place?	FISCAM SC-2.2	Is there a policy that requires a backup power supply?	Are there procedures for establishing and maintaining a backup power supply?	Is a backup power supply in place?	Is the backup power supply periodically tested to verify proper functioning and availability?	Is a backup power supply a standard part of the business environment?
8.1.19	Physical Security	Implementation of physical security controls	Are computer monitors located to eliminate viewing by unauthorized persons?	NIST SP 800-18	Is there a policy that requires computer monitors be located to eliminate viewing by unauthorized persons?	Are there procedures for locating computer monitors to eliminate viewing by unauthorized persons?	Are computer monitors located to eliminate viewing by unauthorized persons?	Is the location of computer monitors periodically reviewed to ensure that viewing by unauthorized persons is eliminated?	Is the location of computer monitors such that viewing by unauthorized persons is eliminated standard business practice?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
8.1.20	Physical Security	Implementation of physical security controls	Is physical access to information transmission lines controlled, including phone and network closets?	NIST SP 800-18	Is there a policy that requires physical access to information transmission lines be controlled, including phone and network closets?	Are there procedures for controlling physical access to information transmission lines, including phone and network closets?	Is physical access to information transmission lines controlled, including phone and network closets?	Are the controls for physical access to information transmission lines, including phone and network closets periodically verified to be effective?	Is control of physical access to information transmission lines, including phone and network closets standard business practice?
8.1.21	Physical Security	Implementation of physical security controls	Are controls in place for transporting and mailing media and printed output?	NIST SP 800-18	Is there a policy that requires specific controls for transporting and mailing media and printed output?	Are there procedures for transporting and mailing media and printed output?	Are controls in place for transporting and mailing media and printed output?	Are the controls for transporting and mailing media and printed output periodically tested to verify effectiveness?	Are controls for transporting and mailing media and printed output part of the standard business practice?
8.1.22	Physical Security	Implementation of physical security controls	Is there physical protection of the media storage vault/library?	NIST SP 800-18	Is there a policy that requires physical protection of the media storage vault/library?	Are there procedures for providing physical protection of the media storage vault/library?	Is there physical protection of the media storage vault/library?	Is the physical protection of the media storage vault/library periodically validated by an independent third party?	Is physical protection of the media storage vault/library standard business practice?
8.1.23	Physical Security	Implementation of physical security controls	Are physical security controls commensurate with the risks of physical damage or access in place?	NIST SP 800-18	Is there a policy that requires physical security controls commensurate with the risks of physical damage or access?	Are there procedures for implementation of physical security controls commensurate with the risks of physical damage or access?	Are physical security controls commensurate with the risks of physical damage or access in place?	Have tests been conducted to validate the use and effectiveness of physical security controls against the risk of physical damage or access?	Are physical security controls commensurate with the risks of physical damage or access integrated into the system development and maintenance process?
8.1.24	Physical Security	Implementation of physical security controls	Are entry codes changed upon termination or reassignment of an individual with access?	FISCAM AC-3.1	Is there a policy that requires all entry codes to be changed upon termination or reassignment of an individual with access?	Are there procedures for changing all entry codes (e.g. facility, computer room, network closet, phone closet)?	Are entry codes changed upon termination or reassignment of an individual with access?	Are there periodic reviews to verify that entry codes are changed upon termination or reassignment of an individual with access?	Is it standard business practice to change entry codes upon termination or reassignment of an individual with access?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
8.2.1	Physical Security	Personal electronic device protection	Are mobile and portable systems protected from unauthorized access?	NIST SP 800-18	Is there a policy that requires protection of mobile and portable systems from unauthorized access?	Are there procedures for protecting mobile and portable systems from unauthorized access?	Are mobile and portable systems protected from unauthorized access?	Is there a periodic validation of the mobile and portable systems protection from unauthorized access?	Is protection of mobile and portable systems from unauthorized access standard business practice?
8.2.2	Physical Security	Personal electronic device protection	Are sensitive data files on mobile and portable systems encrypted (laptops, palm pilots, etc)?	NIST SP 800-14	Is there a policy that requires encryption of sensitive data files on mobile and portable systems (laptops, palm pilots, etc)?	Are there procedures for encrypting sensitive data files on mobile and portable systems (laptops, palm pilots, etc)?	Are sensitive data files on mobile and portable systems encrypted (laptops, palm pilots, etc)?	Is there a periodic third party review to ensure that sensitive data files on mobile and portable systems are encrypted (laptops, palm pilots, etc)?	Is encryption of sensitive data files on mobile and portable systems a (laptops, palm pilots, etc) standard business practice?
8.2.3	Physical Security	Personal electronic device protection	Are mobile and portable systems stored securely?	NIST SP 800-14	Is there a policy that requires secure storage of mobile and portable systems?	Are there procedures for secure storage of mobile and portable systems?	Are mobile and portable systems stored securely?	Is the storage of mobile and portable systems periodically reviewed to ensure appropriate security?	Is secure storage of mobile and portable systems standard business practice?
8.2.4	Physical Security	Personal electronic device protection	Is access to all program libraries restricted and controlled?	FISCAM CC-3.2; FISCAM CC-3.3	Is there a policy that requires restricted and controlled access to all program libraries?	Are there procedures for implementing restricted and controlled access to all program libraries?	Is access to all program libraries restricted and controlled?	Is access to all program libraries periodically reviewed to ensure access is appropriately restricted and controlled?	Is restricted and controlled access to all program libraries standard business practice?
8.2.5	Physical Security	Personal electronic device protection	Are emergency maintenance and repair activities accomplished without adversely affecting IT system security?	NIST SP 800-18; FISCAM CC-2.2	Is there a policy that requires emergency maintenance and repair activities be accomplished without adversely affecting IT system security?	Are there procedures for completing emergency maintenance and repair activities without adversely affecting IT system security?	Are emergency maintenance and repair activities accomplished without adversely affecting IT system security?	Are emergency maintenance and repair activities periodically reviewed to ensure that they are accomplished without adversely affecting IT system security?	Is completion of emergency maintenance and repair activities without adversely affecting IT system security part of the standard business process?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
8.2.6	Physical Security	Personal electronic device protection	Is access by on-site and off-site maintenance personnel appropriately controlled?	NIST SP 800-18	Is there a policy that requires control of access by on-site and off-site maintenance personnel?	Are there procedures for controlling access by on-site and off-site maintenance personnel?	Is access by on-site and off-site maintenance personnel appropriately controlled?	Is access by on-site and off-site maintenance personnel periodically reviewed to ensure appropriate controls are being applied?	Is control of access by on-site and off-site maintenance personnel part of the standard business practice?
8.2.7	Physical Security	Personal electronic device protection	Are devices sanitized prior to removal from the site?	NIST SP 800-18	Is there a policy that requires device sanitization prior to removal from the site?	Are there procedures for device sanitization prior to removal from the site?	Are devices sanitized prior to removal from the site?	Are there periodic third party reviews to ensure that devices are sanitized prior to removal from the site?	Is device sanitization prior to removal from the site standard business practice?
8.3.1	Physical Security	Emanation Controls	Are appropriate controls in place to ensure that sensitive information is not being transmitted from the facility to unauthorized persons?	NIST SP 800-18; FIPS 31	Is there a policy that prohibits transmission of sensitive information from the facility to unauthorized persons?	Are there procedures for preventing transmission of sensitive information from the facility to unauthorized persons?	Are appropriate controls in place to ensure that sensitive information is not being transmitted from the facility to unauthorized persons?	Are controls for preventing sensitive information from being transmitted from the facility to unauthorized persons tested to validate effectiveness?	Are controls to prevent transmission of sensitive information from the facility to unauthorized persons, standard business practice?
8.3.2	Physical Security	Emanation Controls	Are personal electronic devices (cell phones, infrared ports, microwave, etc.) sufficiently controlled to ensure that sensitive information is not available to unauthorized persons?	NIST SP 800-18; FIPS 31	Is there a policy that requires control of personal electronic devices (cell phones, infrared ports, microwave, etc.) to ensure that sensitive information is not available to unauthorized persons?	Are there procedures for controlling personal electronic devices (cell phones, infrared ports, microwave, etc.) to ensure that sensitive information is not available to unauthorized persons?	Are personal electronic devices (cell phones, infrared ports, microwave, etc.) sufficiently controlled to ensure that sensitive information is not available to unauthorized persons?	Are controls for personal electronic devices (cell phones, infrared ports, microwave, etc.) periodically tested to ensure that sensitive information is not available to unauthorized persons?	Are controls for personal electronic devices (cell phones, infrared ports, microwave, etc.) to ensure that sensitive information is not available to unauthorized persons standard business practice?
8.3.3	Physical Security	Emanation Controls	Are appropriate electromagnetic controls part of the network architecture?	NIST SP 800-18; FIPS 31	Is there a policy that requires that appropriate electromagnetic controls be part of the network architecture?	Are there procedures for incorporating electromagnetic controls into the network architecture?	Are appropriate electromagnetic controls part of the network architecture?	Is the network architecture periodically reviewed to ensure that current and appropriate electromagnetic controls are part of the network architecture?	Is it standard business practice to include appropriate electromagnetic controls as part of the network architecture?
8.3.4	Physical Security	Emanation Controls	If wireless transmissions (cell phones, infrared ports, microwave, etc.) are part of the business practice, are appropriate controls in place to ensure data integrity and confidentiality?	NIST SP 800-18; FIPS 31	Is there a policy that requires appropriate controls to ensure data integrity and confidentiality of wireless transmissions?	Are there procedures for controlling data integrity and confidentiality of wireless transmissions?	If wireless transmissions (cell phones, infrared ports, microwave, etc.) are part of the business practice, are appropriate controls in place to ensure data integrity and confidentiality?	Are data integrity and confidentiality controls of wireless transmissions periodically verified to be effective?	Are data integrity and confidentiality controls of wireless transmissions part of the standard business practice?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
8.4.1	Physical Security	Temporary Controlled Facility Controls	Are appropriate physical controls applied to temporary facilities?	NIST SP 800-18; FIPS 31	Is there a policy that requires appropriate physical controls be applied to temporary facilities?	Are there procedures for applying appropriate physical controls to temporary facilities?	Are appropriate physical controls applied to temporary facilities?	Are temporary facility physical controls periodically reviewed to ensure effectiveness?	Are effective temporary facility physical controls standard business practice?
8.4.2	Physical Security	Temporary Controlled Facility Controls	Are appropriate electromagnetic controls applied to temporary facilities?	NIST SP 800-18; FIPS 31	Is there a policy that requires appropriate electromagnetic controls be applied to temporary facilities?	Are there procedures for applying appropriate electromagnetic controls to temporary facilities?	Are appropriate electromagnetic controls applied to temporary facilities?	Are temporary facility electromagnetic controls periodically reviewed to ensure effectiveness?	Are effective temporary facility electromagnetic controls standard business practice?
8.4.3	Physical Security	Temporary Controlled Facility Controls	Is security appropriately considered in the temporary facility selection process?	NIST SP 800-18; FIPS 31	Is there a policy that requires appropriate consideration of security in the temporary facility selection process?	Are there procedures for consideration of security in the temporary facility selection process?	Is security appropriately considered in the temporary facility selection process?	Is the selection of temporary facilities periodically reviewed to ensure that security is appropriately considered?	Is appropriate consideration of security in the temporary facility selection process standard business practice?
8.4.4	Physical Security	Temporary Controlled Facility Controls	Are data integrity and confidentiality taken into consideration when establishing temporary controlled facilities?	NIST SP 800-18; FIPS 31	Is there a policy that requires consideration of data integrity and confidentiality when establishing temporary controlled facilities?	Are there procedures for consideration of data integrity and confidentiality when establishing temporary controlled facilities?	Are data integrity and confidentiality taken into consideration when establishing temporary controlled facilities?	Are data integrity and confidentiality measures in temporary controlled facilities periodically reviewed to ensure effectiveness?	Is consideration of data integrity and confidentiality when establishing temporary controlled facilities standard business practice?
8.4.5	Physical Security	Temporary Controlled Facility Controls	Are structural requirements taken into consideration when selecting temporary controlled facilities?	NIST SP 800-18; FIPS 31	Is there a policy that requires consideration of structural requirements when selecting temporary controlled facilities?	Are there procedures for consideration of structural requirements when selecting temporary controlled facilities?	Are structural requirements taken into consideration when selecting temporary controlled facilities?	Are structural requirements of temporary controlled facilities periodically reviewed to ensure effectiveness?	Is consideration of structural requirements when establishing temporary controlled facilities standard business practice?
9.1.1	IT Security Controls	Identification and authentication	Are users authenticated uniquely by identity?	NIST SP 800-18	Is there a policy that requires users to be uniquely authenticated by identity?	Are there procedures for authenticating users uniquely by identity?	Are users authenticated uniquely by identity?	Are there periodic third party reviews to ensure that users are authenticated uniquely by identity?	Are users authenticated uniquely by identity?
9.1.2	IT Security Controls	Identification and authentication	Is the identification and authentication method (passwords, tokens, biometrics, etc) commensurate with the risk of compromise?	NIST SP 800-18; FISCAM AC-3.2	Is there a policy that requires identification and authentication methods (passwords, tokens, biometrics, etc) to be commensurate with the risk of compromise?	Are there procedures for selecting and using identification and authentication methods (passwords, tokens, biometrics, etc) commensurate with the risk of compromise?	Is the identification and authentication method (passwords, tokens, biometrics, etc) commensurate with the risk of compromise?	Are the identification and authentication methods used (passwords, tokens, biometrics, etc) periodically reviewed to ensure that they are commensurate with the risk of compromise?	Is the use of identification and authentication methods (passwords, tokens, biometrics, etc) commensurate with the risk of compromise standard business practice?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
9.1.3	IT Security Controls	Identification and authentication	Are passwords/ passphrases changed at least every ninety days or earlier if needed?	NIST SP 800-18; FISCAM AC-3.2	Is there a policy that requires changing passwords/ passphrases at least every ninety days or earlier if needed?	Are there procedures for changing passwords/ passphrases at least every ninety days or earlier if needed?	Are passwords/ passphrases changed at least every ninety days or earlier if needed?	Are there periodic reviews to ensure that passwords/ passphrases are changed at least every ninety days or earlier if needed?	Is changing passwords/ passphrases changed at least every ninety days or earlier if needed standard business practice?
9.1.4	IT Security Controls	Identification and authentication	Do passwords/passphrases require alpha numeric, upper/lower case, and special characters?	NIST SP 800-18; FISCAM AC-3.2	Is there a policy that requires passwords/ passphrases contain alpha numeric, upper/lower case, and special characters?	Are there procedures for incorporating alpha numeric, upper/lower case, and special characters into passwords/passphrases?	Do passwords/ passphrases require alpha numeric, upper/lower case, and special characters?	Is there an enforcement mechanism to ensure that passwords/ passphrases require alpha numeric, upper/lower case, and special characters or is there a periodic examination to ensure compliance?	Are passwords/ passphrases containing alpha numeric, upper/lower case, and special characters standard business practice?
9.1.5	IT Security Controls	Identification and authentication	Are passwords/passphrases never displayed when entered?	NIST SP 800-18; FISCAM AC-3.2	Is there a policy that requires passwords/passphrases never be displayed when entered?	Are there procedures for ensuring that passwords/passphrases are never be displayed when entered?	Are passwords/passphrases never displayed when entered?	Are there periodic reviews to ensure that passwords/passphrases are never displayed when entered?	Is it standard business practice that passwords/passphrases are never displayed when entered?
9.2.1	IT Security Controls	Logical Access controls	Is data protected from compromise?	NIST SP 800-18	Is there a policy that requires data be protected from compromise?	Are there procedures for protecting data from compromise?	Is data protected from compromise?	Are periodic tests conducted to ensure that data is protected from compromise?	Is protection of data from compromise standard business practice?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
9.2.2	IT Security Controls	Logical Access controls	If digital signatures are in use, do they conform to specifications of FIPS 186-2?	NIST SP 800-18	If digital signatures are in use, is there a policy that requires digital signatures conform to specifications of FIPS 186-2?	If digital signatures are in use, are there procedures for ensuring that digital signatures conform to specifications of FIPS 186-2?	If digital signatures are in use, do they conform to specifications of FIPS 186-2?	If digital signatures are in use, are tests periodically conducted to ensure they conform to specifications of FIPS 186-2?	If digital signatures are in use, do they conform to specifications of FIPS 186-2?
9.2.3	IT Security Controls	Logical Access controls	Are accounts for inactive users disabled?	NIST SP 800-18; FISCAM AC-3.2	Is there a policy that requires accounts for inactive users be disabled? Does the policy state the timeframe within which this must be accomplished?	Are there procedures for disabling accounts for inactive users?	Are accounts for inactive users disabled?	Are periodic third party examinations conducted to ensure accounts for inactive users are disabled within the required timeframe?	Is disabling accounts for inactive users in a timely manner standard business practice?
9.2.4	IT Security Controls	Logical Access controls	Are vendor supplied passwords replaced upon installation of all hardware and software?	NIST SP 800-18; FISCAM AC-3.2	Is there a policy that requires vendor-supplied passwords be replaced upon installation of all hardware and software?	Are there procedures for replacing vendor-supplied passwords upon installation of all hardware and software?	Are vendor supplied passwords replaced upon installation of all hardware and software?	Are periodic third party examinations conducted to ensure that vendor supplied passwords are replaced upon installation of all hardware and software?	Is it standard business practice to replace vendor-supplied passwords upon installation of all hardware and software?
9.2.5	IT Security Controls	Logical Access controls	Is a user account locked or alarmed after a specified number of failed access attempts?	NIST SP 800-18; FISCAM AC-3.2	Is there a policy that requires locking or signaling an alarm after a specified number of failed user account access attempts? Does the policy specify the number of attempts?	Are there procedures for locking or signaling an alarm after a specified number of failed user account access attempts?	Is a user account locked or alarmed after a specified number of failed access attempts?	Are tests periodically conducted to ensure that each user account is locked or an alarm is signaled after a specified number of failed access attempts?	Is it standard business practice to lock or signal an alarm after a specified number of failed user account access attempts?
9.2.6	IT Security Controls	Logical Access controls	Is separation of duties enforced?	NIST SP 800-18	Is there a policy that requires separation of duties?	Are there procedures for establishing and enforcing separation of duties?	Is separation of duties enforced?	Are tests periodically conducted to ensure enforcement of separation of duties?	Is enforcing separation of duties standard business practice?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
9.2.7	IT Security Controls	Logical Access controls	Do logical access controls restrict users to authorized transactions and functions?	NIST SP 800-18; FISCAM AC-3.2; OMB Cir A-130 App III	Is there a policy that requires that logical access controls restrict users to authorized transactions and functions?	Are there procedures for using logical access controls to restrict users to authorized transactions and functions?	Do logical access controls restrict users to authorized transactions and functions?	Are tests run periodically to verify that logical access controls restrict users to authorized transactions and functions?	Is it standard business practice to use logical access controls to restrict users to authorized transactions and functions?
9.2.9	IT Security Controls	Logical Access controls	Is access to security software restricted to security administrators?	FISCAM AC-3.2	Is there a policy that requires access to security software be restricted to security administrators?	Are there procedures for restricting access to security software to security administrators?	Is access to security software restricted to security administrators?	Are tests periodically conducted by independent third parties to verify that access to security software is restricted to security administrators?	Is restricting access to security software to security administrators standard business practice?
9.2.10	IT Security Controls	Logical Access controls	Are access control lists always cryptographically protected (e.g. encrypted)?	NIST SP 800-18	Is there a policy that requires access control lists to always be cryptographically protected (e.g. encrypted)?	Are there procedures for cryptographically protecting access control lists (e.g. encrypting)?	Are access control lists always cryptographically protected (e.g. encrypted)?	Are tests periodically conducted to ensure that access control lists are always cryptographically protected (e.g. encrypted)?	Is it standard business practice to cryptographically protect access control lists?
9.2.11	IT Security Controls	Logical Access controls	Do all systems remove screen contents from view and require user re-authentication after a nominal period of inactivity?	NIST SP 800-18; FISCAM AC-3.2	Is there a policy that requires all systems to remove screen contents from view and require user re-authentication after a nominal period of inactivity? Is the period of inactivity specified?	Are there procedures for systems to remove screen contents from view and require user re-authentication after a nominal period of inactivity?	Do all systems remove screen contents from view and require user re-authentication after a nominal period of inactivity?	Are there periodic inspections to verify that all systems remove screen contents from view and require user re-authentication after a nominal period of inactivity?	Is it standard business practice for all systems to remove screen contents from view and require user re-authentication after a nominal period of inactivity?
9.2.12	IT Security Controls	Logical Access controls	Are inactive user accounts monitored and removed when not needed?	NIST SP 800-18; FISCAM AC-3.2	Is there a policy that requires removal of inactive user accounts when they are no longer needed? Does the policy stipulate the circumstances under which to remove inactive accounts?	Are there procedures for removal of inactive user accounts when they are no longer needed?	Are inactive user accounts monitored and removed when not needed?	Are there periodic third party examinations to ensure that inactive user accounts are monitored and removed when not needed?	Is it standard business practice to monitor and remove inactive user accounts when not needed?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
9.2.13	IT Security Controls	Logical Access controls	Are internal security labels used to control access to specific information types or files?	NIST SP 800-18; FISCAM AC-3.2	Is there a policy that requires use of internal security labels to control access to specific information types or files?	Are there procedures for use of internal security labels to control access to specific information types or files?	Are internal security labels used to control access to specific information types or files?	Are internal security labels periodically examined to ensure they are used effectively to control access to specific information types or files?	Is it standard business practice to use internal security labels to control access to specific information types or files?
9.2.14	IT Security Controls	Logical Access controls	Is information access restricted at the logical view or field level? (role based access at the application level.)	NIST SP 800-18	Is there a policy that requires restriction of information access at the logical view or field level? (role based access at the application level.)	Are there procedures for restriction of information access at the logical view and field level? (role based access at the application level.)	Is information access restricted at the logical view or field level? (role based access at the application level.)	Are tests performed periodically to verify that information access is restricted at the logical view or field level? (Role based access at the application level.)	Is it standard business practice to restrict information access at the logical view or field level? (role based access at the application level.)
9.2.15	IT Security Controls	Logical Access controls	Do logical access controls restrict users telecommunication access?	NIST SP 800-18	Is there a policy that requires logical access controls restrict users telecommunication access?	Are there procedures for restriction of users telecommunication access using logical access controls?	Do logical access controls restrict users telecommunication access?	Are tests run periodically to verify that logical access controls restrict users telecommunication access?	Is it standard business practice to use logical access controls to restrict users telecommunication access?
9.2.17	IT Security Controls	Logical Access controls	Are insecure protocols (e.g., UDP, ftp) disabled?	NIST SP 800-18	Is there a policy that requires insecure protocols (e.g., UDP, ftp) be disabled?	Are there procedures for disabling insecure protocols (e.g., UDP, ftp)?	Are insecure protocols (e.g., UDP, ftp) disabled?	Are tests periodically conducted to verify that insecure protocols (e.g., UDP, ftp) are disabled?	Is disabling insecure protocols (e.g., UDP, ftp) standard business practice?
9.2.18	IT Security Controls	Logical Access controls	Can users securely access systems remotely?	NIST SP 800-18	Is there a policy that requires remote access by users to be performed using a secure method?	Are there procedures for users to perform secure remote access?	Can users securely access systems remotely?	Are tests periodically conducted to verify that users remote access is performed securely?	Is it standard business practice for users to perform secure remote access?
9.2.19	IT Security Controls	Logical Access controls	Do network connections automatically disconnect at the end of a session?	FISCAM AC-3.2	Is there a policy that requires network connections to automatically disconnect at the end of a session?	Are there procedures for automatically disconnecting network connections at the end of a session?	Do network connections automatically disconnect at the end of a session?	Are tests periodically conducted to verify that network connections are automatically disconnected at the end of a session?	Is it standard business practice to automatically disconnect network connections at the end of a session?
9.2.20	IT Security Controls	Logical Access controls	Are trusted interactions with internal and external entities appropriately restricted?	NIST SP 800-18	Is there a policy that requires trusted interactions with internal and external entities be appropriately restricted?	Are there procedures for appropriately restricting trusted interactions with internal and external entities?	Are trusted interactions with internal and external entities appropriately restricted?	Are trusted interactions with internal and external entities periodically examined to ensure appropriate restrictions?	Is it standard business practice to appropriately restrict trusted interactions with internal and external entities?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
9.2.21	IT Security Controls	Logical Access controls	Is dial-in access monitored to ensure only approved access?	FISCAM AC-3.2	Is there a policy that requires dial-in access be monitored to ensure only approved access?	Are there procedures for monitoring dial-in access to ensure only approved access?	Is dial-in access monitored to ensure only approved access?	Are tests periodically conducted to verify that monitoring of dial-in access is effective in ensuring only approved access?	Is dial-in access monitored to ensure only approved access?
9.2.22	IT Security Controls	Logical Access controls	Is access to telecommunications hardware or facilities restricted and monitored?	FISCAM AC-3.2	Is there a policy that requires restricted access to telecommunications hardware or facilities?	Are there procedures for restricting access to telecommunications hardware or facilities?	Is access to telecommunications hardware or facilities restricted and monitored?	Are periodic examinations performed to ensure that access to telecommunications hardware or facilities is restricted?	Is restricted access to telecommunications hardware or facilities standard business practice?
9.2.23	IT Security Controls	Logical Access controls	Are devices (e.g. firewalls, secure gateways) installed to prevent unintended or malicious access?	NIST SP 800-18	Is there a policy that requires installation of devices (e.g. firewalls, secure gateways) to prevent unintended or malicious access?	Are there procedures for installation of devices (e.g. firewalls, secure gateways) to prevent unintended or malicious access?	Are devices (e.g. firewalls, secure gateways) installed to prevent unintended or malicious access?	Are tests periodically performed to ensure that devices (e.g. firewalls, secure gateways) are effectively preventing unintended or malicious access?	Is the installation of devices (e.g. firewalls, secure gateways) to prevent unintended or malicious access standard business practice?
9.2.25	IT Security Controls	Logical Access controls	Are official records segregated from information made directly accessible to the public?	OMB Cir A-130	Is there a policy that requires official records be segregated from information made directly accessible to the public?	Are there procedures for segregating official records from information made directly accessible to the public?	Are official records segregated from information made directly accessible to the public?	Are there periodic examinations to verify that official records are segregated from information made directly accessible to the public?	Is segregation of official records from information made directly accessible to the public standard business practice?
9.2.27	IT Security Controls	Logical Access controls	Are there logical access controls for inquiry and update capabilities from application program functions, interfacing DBMS, or Data Dictionary facilities?	FISCAM AC-3.2	Is there a policy that requires logical access controls for inquiry and update capabilities from application program functions, interfacing DBMS, or Data Dictionary facilities?	Are there procedures for providing logical access controls for inquiry and update capabilities from application program functions, interfacing DBMS, or Data Dictionary facilities?	Are there logical access controls for inquiry and update capabilities from application program functions, interfacing DBMS, or Data Dictionary facilities?	Are the logical access controls for inquiry and update capabilities from application program functions, interfacing DBMS, or Data Dictionary facilities periodically tested to verify that they are effective?	Are logical access controls for inquiry and update capabilities from application program functions, interfacing DBMS, or Data Dictionary facilities part of the standard business practice?
9.2.28	IT Security Controls	Logical Access controls	If a user account is locked or an alarm is signaled due to failed access attempts, does the reactivation procedure require appropriate identification and authentication of the user?	NIST SP 800-18; FISCAM AC-3.2	Is there a policy that requires locking or signaling an alarm after a specified number of failed user account access attempts? Does the policy specify the number of attempts?	Are there procedures for locking or signaling an alarm after a specified number of failed user account access attempts?	Is a user account locked or alarmed after a specified number of failed access attempts?	Are tests periodically conducted to ensure that each user account is locked or an alarm is signaled after a specified number of failed access attempts?	If a user account is locked or an alarm is signaled due to failed access attempts, is it standard business practice to require appropriate identification and authentication of the user prior to reactivation?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
9.3.1	IT Security Controls	Auditing	Are audit trails used when sensitive inputs/outputs are received/transmitted?	NIST SP 800-18	Is there a policy that requires use of audit trails when sensitive inputs/outputs are received/transmitted?	Are there procedures for using audit trails when sensitive inputs/outputs are received/transmitted?	Are audit trails used when sensitive inputs/outputs are received/transmitted?	Are periodic examinations performed to ensure that audit trails are used when sensitive inputs/outputs are received/transmitted?	Is using audit trails when sensitive inputs/outputs are received/transmitted standard business practice?
9.3.2	IT Security Controls	Auditing	Is inappropriate or unusual activity investigated and appropriate action taken?	FISCAM SS-2.2	Is there a policy that requires that inappropriate or unusual activity be investigated and appropriate actions taken?	Are there procedures for investigating inappropriate or unusual activity and taking appropriate action?	Is inappropriate or unusual activity investigated and appropriate action taken?	Are periodic third party reviews performed to ensure that inappropriate or unusual activity is investigated and appropriate action taken?	Is it standard business practice to investigate inappropriate or unusual activity and take appropriate action?
9.3.3	IT Security Controls	Auditing	Are system actions linked to the user performing the action?	FISCAM SD-2.1; OMB Cir A-130 App III	Is there a policy that requires linking system actions to the user performing the action?	Are there procedures for linking system actions to the user performing the action?	Are system actions linked to the user performing the action?	Are periodic tests conducted to verify that system actions are linked to the user performing the action?	Is it standard business practice to link system actions to the user performing the action?
9.3.4	IT Security Controls	Auditing	Do the security controls detect unauthorized access attempts?	NIST SP 800-18; FISCAM AC-3.2	Is there a policy that requires security controls to detect unauthorized access attempts?	Are there procedures for using security controls to detect unauthorized access attempts?	Do the security controls detect unauthorized access attempts?	Are periodic tests conducted to verify that the security controls detect unauthorized access attempts?	Is the use of security controls to detect unauthorized access attempts part of the standard business practice?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
9.3.5	IT Security Controls	Auditing	Are network access activity logs maintained and reviewed for inappropriate access?	FISCAM AC-3.2	Is there a policy that requires maintaining and reviewing network access activity logs for inappropriate access?	Are there procedures for maintaining and reviewing network access activity logs for inappropriate access?	Are network access activity logs maintained and reviewed for inappropriate access?	Are tests periodically conducted to ensure that network access activity logs maintained and reviewed for inappropriate access?	Is it standard business practice to maintain and review network access activity logs for inappropriate access?
9.3.6	IT Security Controls	Auditing	Is all activity involving access to and modification of sensitive or critical files audited?	NIST SP 800-18	Is there a policy that requires all activity involving access to and modification of sensitive or critical files to be audited?	Are there procedures for auditing all activity involving access to and modification of sensitive or critical files?	Is all activity involving access to and modification of sensitive or critical files audited?	Are tests periodically conducted to ensure that all activity involving access to and modification of sensitive or critical files is audited?	Is it standard business practice to audit all activity involving access to and modification of sensitive or critical files?
9.3.7	IT Security Controls	Auditing	Do the audit trails provide a trace of user actions?	NIST SP 800-18	Is there a policy that requires audit trails to provide a trace of user actions?	Are there procedures for using audit trails to provide a trace of user actions?	Do the audit trails provide a trace of user actions?	Are tests periodically conducted to ensure that the audit trails provide a trace of user actions?	Is it part of the standard business practice for the audit trails to provide a trace of user actions?
9.3.8	IT Security Controls	Auditing	Can the audit trails support after-the-fact investigations of how, when, and why normal operations ceased?	NIST SP 800-18	Is there a policy that requires audit trails to support after-the-fact investigations of how, when, and why normal operations ceased?	Are there procedures for configuring auditing to ensure that audit trails support after-the-fact investigations of how, when, and why normal operations ceased?	Can the audit trails support after-the-fact investigations of how, when, and why normal operations ceased?	Are tests periodically conducted to ensure that audit trails support after-the-fact investigations of how, when, and why normal operations ceased?	Is it standard business practice to use audit trails to support after-the-fact investigations of how, when, and why normal operations ceased?
9.3.9	IT Security Controls	Auditing	Is access to online audit logs appropriately controlled?	NIST SP 800-18	Is there a policy that requires access to online audit logs be appropriately controlled? Are those controls specified?	Are there procedures for appropriately controlling access to online audit logs?	Is access to online audit logs appropriately controlled?	Are tests periodically conducted to ensure that access to online audit logs is appropriately controlled?	Is the process integrated within the system?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
9.3.11	IT Security Controls	Auditing	Are the following parameters always part of any audit entry: user ID, terminal ID, application name, action performed, date, and time?	NIST SP 800-18	Is there a policy that requires the following parameters always be a part of any audit entry: user ID, terminal ID, application name, action performed, date, and time?	Are there procedures for configuring the audit to ensure that the following parameters are always part of any audit entry: user ID, terminal ID, application name, action performed, date, and time?	Are the following parameters always part of any audit entry: user ID, terminal ID, application name, action performed, date, and time?	Are tests periodically conducted to ensure that the following parameters are always part of any audit entry: user ID, terminal ID, application name, action performed, date, and time?	Is it standard business practice to include the following parameters as part of any audit entry: user ID, terminal ID, application name, action performed, date, and time?
9.3.12	IT Security Controls	Auditing	Can the audit trail be queried by user ID, terminal ID, application name, action performed, date and time, or some other set of parameters to run reports of selected information?	NIST SP 800-18	Is there a policy that requires the audit trail be queryable by user ID, terminal ID, application name, action performed, date and time, or some other set of parameters to run reports of selected information?	Are there procedures for configuring the audit to ensure that the audit trail can be queried by user ID, terminal ID, application name, action performed, date and time, or some other set of parameters to run reports of selected information?	Can the audit trail be queried by user ID, terminal ID, application name, action performed, date and time, or some other set of parameters to run reports of selected information?	Are tests periodically conducted to ensure that the audit trail can be queried by user ID, terminal ID, application name, action performed, date and time, or some other set of parameters to run reports of selected information?	Is it standard business practice to enable querying the audit trail by user ID, terminal ID, application name, action performed, date and time, or some other set of parameters to run reports of selected information?
9.3.13	IT Security Controls	Auditing	Do the audit trails provide a chain of custody for secure electronic transactions that identifies sending location, sending entity, action performed, date and time stamp of receipt, and other measures used to ensure the integrity of the document?	OMB Cir A-130	Is there a policy that requires the audit trails to provide a chain of custody for secure electronic transactions that identifies sending location, sending entity, action performed, date and time stamp of receipt, and other measures used to ensure the integrity of the document?	Are there procedures for configuring the audit to ensure that the audit trails provide a chain of custody for secure electronic transactions that identifies sending location, sending entity, action performed, date and time stamp of receipt, and other measures used to ensure the integrity of the document?	Do the audit trails provide a chain of custody for secure electronic transactions that identifies sending location, sending entity, action performed, date and time stamp of receipt, and other measures used to ensure the integrity of the document?	Are tests periodically conducted to ensure that the audit trails provide a chain of custody for secure electronic transactions that identifies sending location, sending entity, action performed, date and time stamp of receipt, and other measures used to ensure the integrity of the document?	Is it standard business practice for audit trails to provide a chain of custody for secure electronic transactions that identifies sending location, sending entity, action performed, date and time stamp of receipt, and other measures used to ensure the integrity of the document?
9.3.14	IT Security Controls	Auditing	Are audit trails sufficiently complete and reliable to validate the integrity of secure transactions?	OMB Cir A-130	Is there a policy that requires audit trails to be sufficiently complete and reliable to validate the integrity of secure transactions?	Are there procedures for configuring the audit to ensure that the audit trails are sufficiently complete and reliable to validate the integrity of secure transactions?	Are audit trails sufficiently complete and reliable to validate the integrity of secure transactions?	Are tests periodically conducted to ensure that the audit trails are sufficiently complete and reliable to validate the integrity of secure transactions?	Is it standard business practice for audit trails to be sufficiently complete and reliable to validate the integrity of secure transactions?
9.3.15	IT Security Controls	Auditing	Can the audit trails be used to prove how documents are controlled upon receipt?	OMB Cir A-130	Is there a policy that requires audit trails be able to prove how documents are controlled upon receipt.	Are there procedures for configuring the audit to ensure that audit trails can be used to prove how documents are controlled upon receipt?	Can the audit trails be used to prove how documents are controlled upon receipt?	Are tests periodically conducted to ensure that the audit trails can be used to prove how documents are controlled upon receipt?	Is it standard business practice for audit trails to be used to prove how documents are controlled upon receipt?

Critical Element Identifier	Topic Area	Subtopic Area	Critical Element Text	Reference	Policy	Procedure	Implemented	Tested	Integrated
9.3.16	IT Security Controls	Auditing	Are there mechanisms to prevent significant events from being arbitrarily or unilaterally retracted from the audit log?	NIST SP 800-18	Is there a policy that requires mechanisms to prevent significant events from being arbitrarily or unilaterally retracted from the audit log?	Are there procedures for using mechanisms to prevent significant events from being arbitrarily or unilaterally retracted from the audit log?	Are there mechanisms to prevent significant events from being arbitrarily or unilaterally retracted from the audit log?	Are tests periodically conducted to verify that mechanisms to prevent significant events from being arbitrarily or unilaterally retracted from the audit log are effective?	Is the use of mechanisms to prevent significant events from being arbitrarily or unilaterally retracted from the audit log part of the standard business practice?
9.3.17	IT Security Controls	Auditing	Are audit logs reviewed frequently for inappropriate or unusual activity?	NIST SP 800-18	Is there a policy that requires frequent review of audit logs for inappropriate or unusual activity? Is the frequency specified?	Are there procedures for frequently reviewing audit logs for inappropriate or unusual activity?	Are audit logs reviewed frequently for inappropriate or unusual activity?	Are there periodic third party reviews to ensure that audit logs are reviewed frequently for inappropriate or unusual activity?	Is it standard business practice to review audit logs frequently for inappropriate or unusual activity?
9.3.18	IT Security Controls	Auditing	Does analysis of audit logs take place in near real time or real time?	NIST SP 800-18	Is there a policy that requires near real time or real time analysis of audit logs?	Are there procedures for near real time or real time analysis of audit logs?	Does analysis of audit logs take place in near real time or real time?	Are there periodic third party reviews to ensure that analysis of audit logs takes place in near real time or real time?	Is it standard business practice to analyze audit logs in near real time or real time?